

Data Access, Security,
Classification and Handling
Student Services Technology and Assessment
Updated May 2007

TABLE OF CONTENTS

Section 1: Objective

Section 2: Data Access and Security

Executive Memorandum C-34 Data Access and Security Policy

FERPA Policy

HIPAA Privacy Regulations

GLBA Guidelines

Section 3: Data Classification and Handling

Roles in Handling Data

Data Classification

Data Handling

Section 4: Securing the Data

Workstation Security

Passwords

Email Security

Internet Security

Application Security

Physical Security

Section 5: Technical Support

Section 6: Questions

Appendix A: Student Services Security Tips

Appendix B: Student Services Data Handling FAQ

SECTION 1: OBJECTIVE

Data is one of the universities most valuable assets. Because staff need to handle sensitive and confidential information, it is necessary to educate employees how to properly secure data. Upon completion of the training, staff should have an understanding of the following concepts:

- Different types of data classifications and how to handle data based on those classifications.
- Policies and guidelines that direct how we must handle and secure data at Purdue University, including data destruction guidelines and policy.

SECTION 2: DATA ACCESS AND SECURITY

C-34 DATA ACCESS AND SECURITY POLICY

Purdue University maintains administrative computing resources, including data and information that are essential to performing University business. These are assets the University has both the right and obligation to manage, secure, protect, and control.

[Data Access and Security Policy: Executive Memorandum C-34](#) applies to administrative computing resources regardless of where they reside.

Access

- To assure employees access to relevant data they need to conduct University business;

Data Security

- To prevent unauthorized access to systems, data, facilities, and networks;

Physical Security

- To prevent any misuse of, or damage to, computer assets or data.

It 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."

To view the complete policy and other information technology policies (i.e. internet, SSN, email), go to http://www.purdue.edu/policies/pages/information_technology/info_tech.html

FERPA POLICY

The Purdue FERPA policy provides a framework for student rights and institutional responsibilities under the "Family Education Rights and Privacy Act of 1974." The policy outlines what rights the student has in regards to his/her education records. It also outlines when education records can be disclosed and to whom. For the complete university FERPA policy, go to http://www.purdue.edu/policies/pages/records/c_51.html

If you or your staff needs access to student data that falls under FERPA, you need to complete the online learning tool available through Student Information Systems at <http://www2.itap.purdue.edu/registrar/training/ferpa/content.cfm>.

Once you have read through the learning tool information, you need to complete the FERPA Quiz. Click the Quiz link at the bottom of the above web location, or go to:

<http://www2.itap.purdue.edu/registrar/training/ferpa/quizenry.cfm> You will be required to retake the sign-off quiz yearly.

HIPAA PRIVACY REGULATIONS

Purdue's Privacy Regulations outlined at http://www.purdue.edu/policies/pages/records/vi_2_1.html are in response to the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA requires that Purdue must preserve the privacy and confidentiality of the protected health information and medical records maintained by its various schools and departments.

If you or your staff has access to data that falls under HIPAA, you need to complete training and sign a confidentiality agreement. Both can be found at <http://www.purdue.edu/push/HIPAA/stafftrng/stafftrng.htm>.

GLBA GUIDELINES

Gramm Leach Bliley was set forth by the Federal Trade Commission. It's intent is to protect personally identifiable information in situations where a consumer has provided information with intent to receive a service. Examples of this are found in the Student Loan area, Bursar check cashing etc. For a complete outline of GLBA go to <http://www.itap.purdue.edu/security/policies/GLBPurdue1.doc>

If you or your staff have access to data that falls under GLBA, you need to complete the online training found at http://www.itap.purdue.edu/security/policies/GLB_Safeguards_Rule_Training_General.pdf

SECTION 3: DATA CLASSIFICATION AND HANDLING

ROLES IN HANDLING DATA

Data Stewards

The Student Data Steward is responsible for facilitating the interpretation and implementation of the data policies and guidelines among their delegates. A data steward is someone who manages data for someone else. Administrative data is not owned by an individual. It is owned by the University and should be shared as appropriate to meet the needs of the University and its customers. Data is to be managed by a data steward as a University resource.

The information owners for data across campus can be found by going to: <http://www.itap.purdue.edu/security/procedures/dataClassif.cfm>

Purdue University Data Security and Access Policy

[Executive Memorandum C-34](#) defines the functional Data Security and Access Policy. This responsibility applies to administrative computing resources regardless of where they reside. It requires that members of the University community act in accordance with this policy, relevant laws, contractual obligations, and the highest standards of ethics. This policy includes centralized and decentralized administration, audit, and control of access and security. An audit trail of the updates made to data is recorded for periodic review by security administrators and/or Internal Audit.

Data Custodian

The [Data Custodian](#) is responsible for implementing the policies and guidelines established by the Data Steward. Responsibilities include physical data storage, back-up and recovery, and the

operation of security and data management systems. All employees are considered Data Custodians for any data in their possession.

DATA CLASSIFICATION

For the purpose of handling data appropriately, data is classified by data stewards into one of the following three categories:

- **Public** -- Information which may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access. Refer to the following web page for information on directory/public information:

Example: reports containing information that are summary reports (enrollment reports, degrees conferred reports, etc), or any report that contains only directory information. Refer to the following web page for more information on public/directory information:

<https://www2.itap.purdue.edu/registrar/training/ferpa/content.cfm>

- **Sensitive** -- Information whose access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection.

Example: PUID; Electronic signature; one record or one cell identification by gender or ethnicity but not personally identifiable information without significant effort. Refer to the following web page for more information:

<http://www.purdue.edu/ssta/datasteward/security/files/Data%20Classified%20Sensitive.pdf>

- **Restricted** -- Information protected because of protective statutes, policies or regulations. This level also represents information that isn't by default protected by legal statute, but for which the Information Owner has exercised their right to restrict access.

Example: SID and SSN information appearing in the data warehouse, restricted directory listings, or any other information that is non-directory information. (Refer to Student [Restricted Data Document](#)).

Data is often classified as Directory Information, or information that is contained in an Educational Record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. The University currently considers the following listed items to be Directory Information: student's name, local and home address, local and home telephone listing, electronic mail address, school, curriculum, classification, enrollment status and credit hour load, dates of attendance, degrees, awards, and honors received, participation in officially recognized activities, sports photograph, and weight, height, and position of members of athletic teams. The University reserves the right to amend this listing consistent with federal law and regulations and will notify students of any amendments by publication in the annual edition of University Regulations.

Data can also be referred to as personally identifiable. Examples of personally identifiable information are gender, date of birth, mother's maiden name, driver's license number, bank account information, and credit card information. This information may be used to steal a person's identity. When Sensitive data is combined with this personally identifiable information, it becomes Highly Sensitive information, and additional steps should be taken to protect it from exposure to individuals who do not have a business need for the information. Refer to the data handling matrix information for how to handle these data.

DATA HANDLING

"Handling" information relates to when you view, update, delete, transfer, mail, store, or destroy data. It also relates to how you transfer the data from one location to another. Data is not always stored electronically. Occasionally it could be paper stored in a filing cabinet or in a binder. Additionally the data could be in a report or in a memo. Therefore, it is important you understand how to handle these situations based on the data's classification.

Based upon how data is classified (Public, Sensitive or Restricted), it may need precautions for handling. The web locations below should be used when you need information related to handling of data. This Student Services links are updated regularly, so you should bookmark them for future reference.

For more information on handling of Student data, refer to the Student Services web page at the following location:

- Handling Printed Student Data
<http://www.purdue.edu/SSTA/datasteward/security/files/Printed.pdf>
- Handling Electronically Stored Student Data
<http://www.purdue.edu/SSTA/datasteward/security/files/Elec%20Stored.pdf>
- Handling Electronically Transmitted Student Data
<http://www.purdue.edu/SSTA/datasteward/security/files/Elec%20Trans.pdf>

SECTION 4: SECURING THE DATA

There are numerous ways in which data can be compromised. Below are ways to secure your workstation, email, passwords and internet access.

WORKSTATION SECURITY

- Lock your workstation when you are away from your desk.
- Shut down the workstation each night. (If you are not supported by the Student Services Zone, contact your technical support to see if this applies to you.)
- Make sure that personal or sensitive data about employees, students, customers, or anyone otherwise affiliated with Purdue is not stored on the workstation hard drive, laptops, tablet PCs, CDs, floppy disks, Blackberrys, or other external devices such as pin drives or any other media subject to confiscation, infiltration or compromise. Personal or sensitive data includes but are not limited to SSN, credit card, and other identification information.
- Store data protected as defined by FERPA, GLBA, HIPAA on departmental servers and not on personal workstations. In addition, storage on servers helps to ensure the integrity of the data with normal backup procedures.
- Empty your Recycle Bin daily.
- Do not store Purdue data on your home computer.
- Delete temporary files.

PASSWORDS

- Always use strong passwords and keep them secret. Visit <http://www.itap.purdue.edu/security/policies/procedures/passguidelines.cfm> for more information.
- 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, email or blackberry.

EMAIL SECURITY

- Check your e-mail "Sent Items" and "Deleted Items" daily for sensitive data.
- Do not open email attachments that you aren't expecting. Especially avoid attachments ending in .exe, .vbs, .pif, .scr, .com, or .bat, and don't unzip files you are not expecting. Don't open the attachment even if it looks like it is sent from someone you know as many viruses can forge, or spoof, the sender's name from names found in address books.
- Never store sensitive personal information such as your bank account information or Social Security numbers on your hard drive of your computer, your e-mail account, or Blackberry.
- Do not email restricted data. Note: Refer to Student Restricted Data document. The preferred method of delivery for restricted data is hand delivery.
- Never comply with requests for personal information from an e-mail or phone call unless you initiated the contact. These are often scams trying to steal personal information.

INTERNET SECURITY

- Do not download software such as screensavers, games, or other programs from unfamiliar or unverified sources. These can harbor computer viruses or open a "back door," giving others access to your computer.
- Delete temporary internet files.
- Turn off auto-complete. It stores information such as usernames and passwords.

APPLICATION SECURITY

- Social Security Numbers are extremely sensitive information. They are classified as "restricted" data. Written permission is needed to have access to SSN in DSS or SAS Share. To obtain permission, contact the Student Services Data Steward to complete documentation outlining your legal need for access to these data.

PHYSICAL SECURITY

- Sensitive and Restricted data should be stored in secured locations (i.e. locked filing drawers and cabinets).

SECTION 5: TECHNICAL SUPPORT

If you do not receive technical support from the Student Services Zone, below is a list of questions that you should discuss with your own technical support.

- How should I close down my workstation at the end of the day? Log Off or Shut Down?
- How can I save my files onto a secured server?
- Are there any automatic scripts run on my machine to clean out temp files for I.E. and Outlook attachments? If not, how do I manually clean them off?
- Does the Recycle Bin on the computer get emptied automatically or do I need to delete the files there? If so, how do I delete them?

- Can my Microsoft Applications and possibly other applications be automatically set up to default somewhere other than my workstation. If not, how do I do this manually?

SECTION 6: QUESTIONS

Questions regarding the classification or handling of data should be directed to the Student Services Data Steward. Questions regarding the interpretation of policies and practices should be directed to your Director. Questions regarding workstation security should be directed to the Student Services Zone Manager or your own technical support staff.

APPENDIX A - STUDENT SERVICES SECURITY TIPS

Security is Everyone's Responsibility!

Passwords:

Never share your password.

A good password has the following qualities:

- It is at least seven characters long
- It is easy enough for you to remember that you do not need to write it down
- It includes both upper and lower case letters
- It includes both digits and/or punctuation characters as well as letters
- It does not use proper names, such as, Washington, Harry, Bob, etc.
- It does not use personal information, such as, your phone number, street address, pet's name, etc.
- It is not a dictionary searchable word in any language

Keep it Secure!

- Lock your workstation when away from your desk.
- Do not Share Your Password.
- Do not Log in for some one else.

APPENDIX B - STUDENT SERVICES DATA HANDLING FAQ'S

Q1. Is it considered secure to email a spreadsheet with restricted or sensitive information attachment if its password protected?

A1. The answer is No, per ITaP Security. An attachment must be encrypted to be considered secure to email sensitive information.

Q2. Is it considered secure to have a shortcut on the desktop that points to a file on the network if the file contains sensitive information?

A2. The answer is No, per ITaP Security and Privacy. SSTA suggests placing shortcuts in your home directory (H:) so they are better secured on the network.

Q3. Is it okay to send SIDs through campus mail on CD/disk?

A3. The answer is No, per Rob Stanfield - ITaP's Director of the new Identity and Access Management Office. "There's too much risk in it getting lost or stolen. Assuming this is for data transfer, I'd suggest you have it hand-delivered to the recipient or to an assistant on their behalf and the media destroyed once the transfer is complete."

Q4. Is it okay to send a CD with SIDs to a third party through a delivery service such as FedEx?

A4. The answer is No, unless . . . per Rob Stanfield. An exception is allowed if the contents of the CD are encrypted prior to shipping.

Q5. How do I find out what my PUID is?

A5. Your PUID is printed on the Purdue University ID Card and is contained on the magnetic strip on your card. You can all look up your PUID by accessing your Purdue University directory information at <http://www.itap.purdue.edu/directory/>. Choose the option that allows you to "Edit Personal Directory Entry." You will need to log in with your Career Account information in order to view your detailed directory information. Your PUID is listed near the bottom of the directory information. Students can also look up their PUID on SSINFO. Beginning October 2005 all new employees will receive a letter containing their PUID shortly after they begin employment with Purdue University. Current Purdue employees received a letter in October 2005 containing this same information.

Q6. Is PUID considered restricted or sensitive?

A6. The intent of PUID is to make it a number that has no value outside of Purdue University. However, there are certain privileges that are associated with your PUID, and although the number isn't considered restricted, it IS considered to be sensitive information. The PUID, when associated with other authentication credentials, could grant access to the student record information, so it is important that it be considered as sensitive data and that it not be displayed in a public manner. As a result, the data handling rules for sensitive data apply in this case.

Q7. Can PUID be used for posting grades?

A7. No, it can not. Posting of grades with any information that could result in the student being personally identified is not permitted. Please refer to the following directive from the Office of the Provost:

http://www.purdue.edu/provost/shtml/grad_post.shtml

Q8. Can PUID be displayed on mailing labels?

A8. No. Again, the PUID, when associated with other authentication credentials, could grant access to the student's confidential information, so it is important that it be considered as sensitive data and that it not be displayed in a public manner. As a result, the data handling rules for sensitive data apply in this case.

Q9 Can I save restricted data if I have access to it?

A9 Restricted or sensitive data about employees, students, alumni, customers, or anyone otherwise affiliated with Purdue should only be stored on secure university servers. Never save restricted data to your desktop or hard drive. Personal or sensitive data include but are not limited to SSN, PUID, credit card information, and other personal identification information like birthdates, maiden names, etc.

Q10 Can I transmit PUID via an email message?

Sensitive data may be transmitted in email messages as long as the data does not permit personal identification of the individual. For example, PUID could be used in an email, but it should not be combined with other data that could result in personally identifying the individual.