

Shippensburg University

Information Security Plan

Table of Contents

Shippensburg University Information Security Plan

- I. Information Security Plan
- II. Appendices
 - A. Information Systems Plan
 - B. Admissions Office
 - C. Registrar's Office
 - D. Extended Studies Office
 - E. Ezra Lehman Memorial Library
 - F. Financial Aid Office
 - G. Student Accounts Office
 - H. Academic Success Program
 - I. Social Equity Office
 - J. Disability Services Office
 - K. Dean of Students Office
 - L. Etter Health/Counseling Center
 - M. Public Safety Office
 - N. Human Resources Office
 - O. Contracting Office
 - P. Procedure for Responding to Right-to-Know Requests.
 - Q. Confidentiality Statements

Information Security Plan¹

Shippensburg University

I. The designated employees for the coordination and execution of the information security plan are the Vice President for Information Technologies and Services and the Associate Provost and Dean of Graduate Studies of Shippensburg University. All correspondence and inquiries should be directed to the Office of the Vice President for Information Technologies and Services.

II. The following areas have been identified as relevant when assessing the risks to customer information and the following individuals have been identified as responsible for securing customer information in accordance with all privacy guidelines

Information Systems / System Failures	VP for Info Technologies & Services
Admissions	Dean of Admissions
Registrar's Office	Registrar
Extended Studies	Dean of Extended Studies
Ezra Lehman Memorial Library	Dean of Library and Multimedia Services
Financial Aid Office / Student Loans	Director of Financial Aid
Student Accounts Office	Bursar
Dean of Students Office	Assoc. VP and Dean of Students
Etter Health/Counseling Center	Assoc. VP for Student Affairs
Employee Training and Management	Staff Development Manager
Contracting	Director of Purchasing and Contracting
Act 101 Grant/Grant Accounting	Dean, Academic Programs & Services
	Exec. Director, Sponsored Programs
Social Equity Office	Director of Social Equity
Public Safety Office	Director of Public Safety

III. The Vice President for Information Technologies and Services will coordinate with the relevant areas to monitor and maintain the information security program. The Associate Provost and Dean of Graduate Studies will provide guidance in complying with all privacy regulations. A written security policy that details the information security policies and processes will be maintained by each relevant area and will be made available to the Associate Provost and Dean of Graduate Studies upon request. In addition, the Information Technologies and Services Division will maintain and provide access to policies and procedures that protect against any anticipated threats to the security or integrity of electronic customer information and that guard against the unauthorized use of such information.

IV. Shippensburg University will select appropriate service providers that are given access to customer information in the normal course of business and will contract with them to provide adequate safeguards. In the process of choosing a service provider that will have access to customer information, the evaluation process shall include the ability of the service provider to safeguard customer information. Contracts with service providers shall include the following kinds of provisions:

¹ Adapted from **Model Security Plan #1**, submitted by a NACUBO member institution, April 23, 2003

An explicit acknowledgement that the contract allows the contract partner access to confidential information;

A specific definition of the confidential information being provided;

A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;

A guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;

A guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information;

A provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract;

A stipulation allowing the entry of injunctive relief without posting bond in order to prevent or remedy breach of the confidentiality obligations of the contract;

A stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Shippensburg University to immediately terminate the contract without penalty;

A provision allowing auditing of the contract partners' compliance with the contract safeguard requirements; and

A provision ensuring that the contract's protective requirements shall survive any termination agreement.

For exact wording and the complete set of provisions, see "Shippensburg University Confidential Information Addendum" (Appendix J). This addendum amends and is incorporated into agreements between service providers and Shippensburg University, contractually requiring them to implement and maintain safeguards.

V. This information security plan shall be evaluated and adjusted in light of relevant circumstances, including any material changes in the University's business arrangements or operations, or as a result of testing and monitoring the safeguards. An annual risk assessment will be completed by each relevant area and coordinated by the Associate Provost and Dean of Graduate Studies. The individuals identified in Section II as responsible for securing customer information shall serve as the Information Security Risk Assessment (ISRA) Team. The Vice President for Information Technologies and Services and the Associate Provost and Dean of Graduate Studies will serve as co-chairs. The ISRA Team shall be responsible for the evaluation of the risk of new or changed business arrangements. Periodic auditing of the University's (as well as each relevant area's) compliance with these security and privacy regulations will be completed per the schedule developed by the State System Internal Audit Group.

Approved by: President Ceddia

Approved by: President's Cabinet May 10, 2004

Effective: May 22, 2003

Appendices

- A. Information Systems Plan
- B. Admissions Office
- C. Registrar's Office
- D. Extended Studies Office.
- E. Ezra Lehman Memorial Library
 - 1. Safeguarding Procedures
 - 2. Pennsylvania State Law, Act 1984-90, Section 428
- F. Financial Aid Office
- G. Student Accounts Office
- H. Academic Success Program
- I. Social Equity Office
- J. Disability Service Office
- K. Dean of Students Office
 - 1. End User License Agreement (EULA)/Software Download
 - 2. End User License Agreement (EULA)/User Registration
- L. Etter Health/Counseling Center
 - 1. Etter Health Center – Authorization for Release of Information to Parent(s) or Guardian(s)
 - 2. Etter Health Center – Authorization for Release of Information
 - 3. University Counseling Center – Audio/Videotape Release Form
 - 4. University Counseling Center – Group Member/Leader Confidentiality Statement
- M. Public Safety Office
- N. Human Resources Office
 - 1. Employee Training and Management
 - 2. Communication/Education Plan
 - 3. FERPA Awareness and Training

4. Student Employee Confidentiality
 5. State System Mutual Non-Disclosure Agreement
- O. Contracting Office
1. Confidential Information Addendum
 2. Example: National Student Clearinghouse
- P. Procedure for Responding to Right-to-Know Requests
- Q. Confidentiality Statements
1. SAP Timekeepers
 2. Common Confidentiality Statement

Rev. 6/1/06; 7/07

Information Security Plan for Information Systems
Gramm-Leach-Bliley Act (FTC)
Shippensburg University

Access control:

Student computer records are stored on an UNISYS Clearpath IX5600 and a secured Oracle Sun server. These systems are password protected. The transactions are grouped and authorized by function such as admissions, student accounts, academic records, and financial aid.

The Unisys system uses the SU network system to communicate between the mainframe system and the staff using InfoConnect on personal computers. This system is protected by a firewall and users must log onto this network before they can use the SIS system. Users need a user identification, password and roles to access the Oracle Sun server.

Physical Security:

Offices are locked when staff members are not present in the office. Doors to the Computer Room are always locked. Student files are locked in secured cabinets in the Academic Records Office.

Encryption:

The web student registration system uses encryption when communicating with students over the campus intranet.

Change management process:

The computer systems are stored in an editing system that records the changes that are made to computer programs. This system is also used for system documentation and system run instructions. Access to this system is controlled by the network passwords and a password to login to the system.

Dual control:

The organization structure of the administrative offices and the computer system provide segregation of duties.

Monitoring systems and procedures:

All changes to student records are logged on a logging file and include the transaction information, computer terminal operator, date and time. The logging file is copied each day and is kept indefinitely.

Incident response program:

The transaction log is reviewed any time there is a question on how data on a student's records were changed.

Disaster recovery program/Backup procedures:

Computer database files are backed up every evening and stored in a fireproof safe on site. Every weekend, a complete mainframe dump is done and sent off site to another building on campus. Backups are done on all of the university servers. Once a week copies of these server files are moved to another building site on campus. Some of these files are restored weekly to test the validity of the backup tapes.

Passwords:

Users are prompted to change their passwords every 30 days. All information systems have a process for a user to change their password anytime.

Limited Access:

Access is limited to users. Users only see what information is necessary for them to perform their position functional duties. Faculty and students do not access the mainframe where transactional information is recorded. Instead, faculty and students must login to the University's web site to get information that pertains to them individually.

Documented Procedures:

Procedures are written and stored on a share drive for individuals who need access and are authorized to view the procedure documents.

Equipment maintenance:

Regular routine software maintenance is performed on all of the university's servers. Upgrades are scheduled at times that least impacts the university's operations. Hardware maintenance is done through individual contracts with vendors. This includes contracts for personal computers, servers, mainframe and any other technical equipment.

Employee Training:

Employee training is done periodically when new applications or changes in processes warrant training. Training is done in the computer labs to allow users to have "hands on" training. Technical staff training may involve staff being sent off-campus to receive training for a particular application.

Computer Strategy:

Strategy is determined by reviewing computer services needs by the ITS Division staff. This group meets regularly to determine plans and needs for technical equipment and software upgrades. Scheduling of upgrades is done by planning when the upgrades will least impact the university. Computer equipment is purchased and replaced on a computer life cycle determined by the university.

COMPUTING TECHNOLOGIES CENTER

ARK ACCOUNT REQUEST

Please reply to this email indicating that you agree to paragraphs below. When you reply, be sure to select "Include Message Received from Sender" and include the words "I agree" in the message body. The account will be added after I receive your reply.

Name:

User ID:

Password:

Please change your password using the following page:

<http://Info.ship.edu/chng-arkpw.cgi>

To create a personal webpage, you will need to add a directory called "public_html" in your ark home directory. All web files must be stored within the public_html directory. The files may be transferred with FTP. The hostname of the FTP server is "ark.ship.edu".

Your personal web page URL will be <http://www.ship.edu/~>.

I hereby affirm that I will not make private use of the Shippensburg University computer system for personal gain be it for the services outside the university, for honoraria, gifts, gratuities, or any other form that can be construed as payment for services rendered.

I affirm that I will be the only person who will use this ID to access the ARK computer system at Shippensburg University.

Please contact the Computing Technologies Center, if you have any questions concerning outside services.

Thank You.

COMPUTING TECHNOLOGIES CENTER
Request for ID to SAP Shared Administrative Systems

SAP ID's are created by the Administrative Assistant in the Computing Technologies Center (CTC). All users are assigned SAP roles that are determined by the Administrative Services and Human Resources Offices. Based on the employee's position assignment, all SAP roles associated with SAP FI-MM are approved by the Associate Vice-president of Administration and Finance. All SAP roles associated with SAP HR/Payroll are approved by the HRIS Manager in Human Resources.

When an employee leaves the university or changes position within the university, these offices notify the CTC of the changes that are to take effect. When a new employee is assigned to position, the SAP roles from the previous employee had are added to the new employee. When an employee changes to a different university position, SAP roles from the previous position are removed and new SAP roles are assigned to the current employee's position.

There are instances when other SAP processes are assigned SAP roles. SAP Security Administration, SAP Business Warehouse (BW) and SAP Ad Hoc Reporting roles are assigned by System Technology Consortium (SyTEC) Information Systems Security Lead.

COMPUTING TECHNOLOGIES CENTER
Access to Oracle Shippensburg University Business Datamart

Shippensburg University provides community access to information through the Web. Currently there are four types of community access; Student Information System (SIS), Faculty Information System (FIS), Department Information System (DIS) and Administrative Information System (AIS).

All students have access to SIS. The SIS system provides students with access to information pertaining to their academic records and allows them to do online scheduling. Students are required to use a userid and password to access their information. When a student leaves the institution, they no longer have access to the Datamart. All students have the same access as all other students.

All faculty have access to FIS. The FIS system provides faculty with access to information on advising students, class lists, grade reporting, and evaluations. Other information is provided here also. Faculty are required to use a userid and password to access the system. Faculty are added by the Web Development team from a list provided by the Provost's Office. All faculty have the same access as all other faculty.

Department chairpersons and secretaries have access to DIS. The list of these individuals is maintained by the Registrar's Office. The Web Development team adds the roles to the individual. Users are required to use a userid and password to access the system. All departments have the same access as other departments.

University staff employees have access to the AIS. The AIS system provides information to web systems designed by the Web Development team. It also provides specific reports to named individuals that can not be included in the FIS or DIS systems. Users are required to use a userid and password to access the system. Roles are assigned so that only the information the user needs is displayed. Users of this system do not see the same applications that other users might see in this area.

With the exception of students, all users are added, changed, removed from the web systems by CTC when properly notified. Faculty and staff userid's are created using the user's e-mail address.

Shippensburg University-Office of Admissions

Safeguarding Procedures

Gramm-Leach-Bliley Act

I. Staff/Employee Management

The Office of Admissions strives to keep student information confidential and private. There are annual training sessions and daily reminders given to the office staff to ensure the safeguard procedures are enforced. Student workers (Graduate Assistants/Work Study Students/Interns) are also briefed of the confidentiality procedures and courses of action if a student is caught using or accessing information inappropriately. All student workers are required to sign a confidentiality agreement prior to starting work in the Office of Admissions. (Enclosed)

II. Physical Security

MAIN OFFICE Old Main 105: There are two doors leading into the main Admissions Office that are open during normal business hours. Anyone entering through those doors must pass the front receptionist desk, which is always staffed. This allows monitoring of individuals entering and exiting the office. The other doors leading into various parts of the Admissions Office are locked 24 hours a day. After normal business hours, all doors are locked and can only be opened with master key. The In-Counselor is responsible for locking the Office of Admissions at the close of business.

OFFICE SUITE Old Main106 : There is one door leading into the 106 Office Suite and the last counselor leaving for the day locks this door at the close of business. If the counselor leaves their office for an extended period of time, they are to lock their office. The counselors monitor all individuals entering into the suite.

2nd FLOOR ADMISSIONS OFFICE: There are 3 doors entering into the 2nd floor office. Two doors are open during business hours and third is always locked. The staff is responsible for monitoring who is entering the office. During regular business hours, if everyone is out, it is the responsibility of the last person leaving to lock the office. All doors are locked at the end of the day.

III. Student Applications/Files

Access to student paper files and the online database of applicants is limited to the Admissions staff and student workers. Each individual has specific access to the database information by use of a password. All paper files are stored in filing cabinets when not being used. If a student file is removed from the filing cabinets, it must be signed out and is the responsibility of the individual to keep the application safeguarded. Applications must always remain in the Admissions office at all times.

No one is allowed to remove an applicant's file from the office (take home, etc). If a file is removed from the Admissions Office (ex. To the President's Office), it must have an approval from the Associate Dean or Dean of Admissions.

IV. Checks

The support staff handles all checks that are received by mail in the Admissions office. The check remains with the student file until processed. Once processed, it would be immediately sent to student accounts. If there is any delay time in processing, the checks are securely placed in a locked filing cabinet.

V. Releasing Applicant Information

TELEPHONE: The Office of Admissions has a policy of not releasing any specific information over the phone. Information such as grades, application status, SAT scores and other personal information can only be verified. Status of applications can be checked online by applicants through the University Web Site. Information requested by parents occurs most frequent; however we encourage them to speak to their son or daughter to get that information.

IN PERSON: If a meeting occurs with a student and the staff member is sure of identity, most information will be released.

VI. Reports

Reports are delivered to the Admissions Staff via e-mail. If a report is not going to be used or needed, the report is to be deleted from their computer. If a printed copy of the report is required and it has personal information such as social security numbers, it is to be treated like a student file and safeguarded from others. It should be filed in filing cabinets during use and shredded when done.

VII. Shredding of Documents

The Office of Admissions has two locations where documents are placed to be shredded. The locations are out of the way from visitors entering in the office. Information with social security numbers is always shredded after use.

VIII. Credit Card Information

Credit card numbers and information shall be treated similar to check procedures. All credit card information will remain in the file until sent to Student Accounts for processing. If a student walks in the Admissions and wants to pay with credit card, they are sent to the Student Accounts office to pay and student returns with receipt.

IX. FERPA

The Registrars Office has trained the Office of Admissions on FERPA guidelines. Changes or updates are immediately communicated to the staff.

**Shippensburg University
Registrar's Office
Safeguarding Procedures
Gramm-Leach-Bliley Act**

Employees Management

When hired, all employees in the Registrar's Office are briefed on FERPA and privacy rights of students by the Registrar. These issues are also discussed at staff meetings and retreats. Publications of current court cases and FERPA debates are regularly shared with staff.

Student employees are also briefed on FERPA and privacy issues when hired. Students are required to sign the agreement that the Information Security Committee designed. FERPA and privacy issues are discussed at the Registrar's Office mandatory student meeting held each semester. Any breach of this agreement results in the loss of employment and possible judicial action by the university.

Office Safeguards

Paper Documents and Student Files:

Students' files are kept in filing cabinets and have limited access. The cabinets are closed at night, and the office is locked. Only full time employees have key access to the office. Files that are stored in the basement are behind locked doors and have limited access. Staff and faculty are permitted access to these files on a need to know basis.

Any paper documents with a student's Social Security Number or academic record are put in the shredding can, and the office personnel shred these documents.

Phone Contact:

A student's record will not be discussed on the phone.

Service at the Counter:

The Registrar's Office requires identification before any information will be given to a student at the counter. Confidentiality is difficult in this office with so many customers at the counter at the same time. Employees ask students to write their SSN on a piece of paper instead of asking them to repeat it. If a student is uncomfortable discussing their record at the counter, provisions can be made to have the discussion in a more private environment.

School Seal and Transcript Paper

The school seal and security transcript paper are locked in a cabinet at night.

Credit Cards

The Office of the Registrar collects this data, and it is hand-delivered to the Student Accounts Office on the same day it is received. If delivery is not possible that day, the information is kept in a locked and secure environment until it can be transferred to the Student Accounts Office. Copies of these forms with credit card information are kept in filing cabinets.

Computer Access

All employees of the Office of the Registrar are given access to only those transactions on the student mainframe necessary to perform their duties. Student database access is approved only for other employees who have a need to know. Access to the mainframe and online information is password protected.

February 17, 2004
rev: June 1, 2007

Shippensburg University – Extended Studies
Safeguarding Procedures
Gramm-Leach-Bliley Act

Employee Management

All employees of the Office of Extended Studies are briefed on the privacy rights of students and FERPA. The team makes every effort to maintain security, confidentiality and integrity of customer (non-credit) and student (credit) information.

Student employees are briefed on FERPA and privacy issues when hired and must sign a confidentiality statement, a breach of which would result in loss of employment and possible judicial action.

Office Safeguards and Physical Security

Paper Documents

The office is kept locked at night. Only office employees and essential university employees have key access.

Paper documents are stored in office file cabinets and are shredded when no longer used. All trash and any documents containing social security numbers are shredded as well.

Checks and cash are kept in a locked file overnight. Only a few office employees have access to the locked file.

Credit Cards

Credit card information may be received for credit or non-credit programming over the phone, in person, through the mail or via the Internet. When possible, credit card information is delivered to the Student Accounts Office (credit operation) or Accounts Receivable/Foundation (non-credit operation) in the same day it is received. Credit card information is hand-delivered to the Student Accounts Office; it is never placed in university mail. Any documents or receipts containing credit card numbers are stored in a locked file cabinet. After the credit card information is forwarded to Student Accounts, any documents, including trash or unnecessary paperwork, containing credit card information are shredded immediately.

Computer Access

Employees in the Office of Extended studies are given access to only those transactions on the student mainframe or the WERKS (WEDnetPA mainframe for non-credit operation) necessary to perform their duties. Access to the mainframe and online information as well as the WERKS system are password protected. Access to the extended studies database is limited to

extended studies personnel and other staff specifically with a need to know. The extended database is password protected.

Phone contact

A student's (credit) or customer's (non-credit) record will not be discussed over the phone.

Service at the Front Desk

The Office of Extended Studies requires identification before any information will be given to anyone in person.

Shippensburg University
Ezra Lehman Memorial Library
Safeguarding Procedures
Gramm-Leach-Bliley Act

Employees Management

Library personnel and student records are not discussed over the telephone. Should a library patron call inquiring about the status of their record as it relates to borrowing privileges or access to licensed databases from off-campus, library faculty and staff are only permitted to verify information provided by the patron. Questions concerning inaccurate patron information are referred to the Head of Access Services.

New library employees are briefed on the privacy rights of students and are informed of standard university and library practice. Privacy rights are reviewed at the first faculty and staff meetings of each new academic year and are addressed throughout the year as needed.

Student employees are informed of privacy rights when hired. At that time undergraduate and graduate employees are required to sign the Student Employee Confidentiality Agreement. Privacy rights are discussed as a part of mandatory training at the beginning of each semester and are reviewed at student training meetings. Students are advised that a breach of the confidentiality agreement may result in the loss of employment and possible judicial action by the university.

Office Safeguards

Paper Documents and Personnel Files:

All personnel files (faculty, staff, and student) are kept in a filing cabinet located in the Dean's Office. The filing cabinet is locked at all times, with key access available only to the Dean of Library and Media Services and the Dean's Secretary. The Dean's office is locked at night and throughout the day when the Dean is not present. Faculty and staff are permitted access to personnel files on a need to know basis.

All paper documents displaying Social Security Numbers are shredded at the time of disposal.

Telephone Contact:

Circulation Desk Service:

Voyager charge and discharge screens, which are used to circulate materials at the Circulation Desk, are displayed using a generic student assistant login that grays out the patron record button. Patron records can be accessed in this mode via a patron name search but student workers are instructed never to search in this manner since library policy specifies that patrons must present a university ID to access the system.

Computer Access:

Access to student information in the Voyager Patron Database is restricted, through the Systems Administration module, to designated faculty and staff. Only faculty and staff working in the Access Services and Reference Departments can view patron information. Access to patron information is password protected.

Should a patron inquire about the status of their record as it relates to borrowing privileges or access to licensed databases from off-campus, library faculty and staff are only permitted to verify information provided by the patron. Patrons are asked to write their Social Security Number on a piece of paper. The paper is destroyed in front of the patron before they leave the Circulation Desk. PCs are positioned on the Circulation Desk in such a way that patrons cannot view patron record screens when they are displayed. Questions concerning inaccurate patron information are referred to the Head of Access Services.

If a patron is uncomfortable discussing their record at the Circulation Desk, they will be invited to move to a staff work area behind the Desk.

Pennsylvania State Law. PA Act 1984-90, Section 428.

Library Circulation Records--Records related to the circulation of library materials which contain the names or other personally identifying details regarding the uses of the State Library or any local library which is established or maintained under any law of the Commonwealth or the library of any university, college or educational institution chartered by the Commonwealth or the library of any public school or branch reading room, deposit state, or agency operated in connection therewith, shall be confidential and shall not be made available to anyone except by a court ordinance in a criminal proceeding.

Shippensburg University
Financial Aid Office
Safeguarding Procedures

Employee Management

Department Employees

- New employees are briefed regarding security and confidentiality of information for employees, students and applicants.
- Related issues are discussed regularly at staff meetings and weekly meetings with the Director.
- Publications with related articles and information are shared with staff members.

Student Employees

- Student employees in the Financial Aid Office are asked to sign a confidentiality agreement.
- The student supervisor will discuss the importance of confidentiality and the consequences of breach of agreement with the student.

Office Safeguards

Paper Documents and Files in Office

- Confidential documents are stored in cabinets and drawers in each individual office.
- Paychecks are sealed prior to delivery to the office and are kept in file cabinets which can only be accessed by office employees.
- The office is kept locked during non-work hours. Only office employees and essential University employees have key access.
- Any paper documents with a student SSN or other confidential information that is no longer needed is shredded.

Paper Documents and Files in Archives

- Archived files are locked in a separate storage space which can only be accessed by office members.
- Records or files that are purged are shredded before disposal.
- All student Financial Aid folders are destroyed 5 years after separation from the University.

Phone Contact

- A student's record and information will not be discussed on the phone unless proper identification is provided by the caller through an SSN or other qualifying information.
- Office personnel will check Mainframe and PHEAA to see if the student has asked for information restrictions before discussing information over the phone.

Service at the Front

- The Financial Aid Office uses a SSN as identification before any information will be given to a student at the counter.
- Confidentiality is difficult in this office given the possibility of multiple customers at the front counter.
- If a student or parent is uncomfortable discussing their record at the front counter or the front counter staff determines the need for a more private environment, appropriate provisions will be made to have the discussion in a more private environment.

Computer Access

- Access to mainframe, PHEAA, and online information is password protected.
- Employees of the Financial Aid Office are given access to PHEAA and Mainframe necessary to perform their duties.
- Student use of PHEAA and Mainframe is limited and access is provided by their supervisor on an individual basis.

4/1/04

Shippensburg University – Student Accounts Office

Safeguarding Procedures

Gramm-Leach-Bliley Act

Employee Management

Student Accounts Staff must continue to strive to maintain security, confidentiality and integrity of customer information. All employees must attend University training, including new employee training, and annual office training to reinforce existing and new safeguarding procedures.

Student employees in the office must sign a confidentiality statement, a breach of which would result in loss of job and possible judicial action.

Office Safeguards and Physical Security

Paper Documents

The office is kept locked at night. Only office employees and essential university employees have key access. The door adjoining Student Accounts and the Financial Aid Office can be accessed only on the side of Student Accounts.

Bills, reports and other paper documents are stored in office file cabinets and are shredded when no longer used. All trash, receipt copies and any documents containing social security numbers are shredded as well. For audit purposes, all financial data must be kept for 7 years. These documents are kept in the Old Main basement in a locked room, accessible only with a key kept in the Office of the Assoc. VP of Admin and Finance. After 7 years, all documents are shredded.

Checks and cash are kept in a locked safe over night. Only several office employees have access to the combination to unlock the safe.

Credit Cards

Credit card information may be received over the phone, in person, through the mail or via the Internet. Information may be received directly in the Student Accounts Office or through other offices. Any documents or receipts containing credit card numbers or account information are stored in file cabinets or the office safe and are kept locked after hours. As with other financial information, these documents are stored for 7 years in a locked room in the basement and are shredded at the end of that period.

Other office that receive credit card information and account numbers (such as, but not limited to, the Registrar's Office, Admissions, Dean of Students, Extended Studies, Conferences Office and University Police) must follow proper safeguarding procedures when handling that information. Whenever possible, credit card information should be delivered to the Student Accounts Office in the same day that it is received. If not, info must be kept in a locked and secure environment until such time that it can be transferred to Student Accounts. Any trash or unnecessary paperwork containing credit card data should be shredded immediately. Information should be hand-delivered to the Student Accounts Office, never placed in university mail.

Credit cards are also processed via the Internet, currently through Yourpay. These are processed through a secure server. Yourpay is password-protected, with only a limited number of staff having access.

Account Information on Student Information System

See *Information Security Plan for Information Systems* for information on university computing safeguards.

Access to students' accounts on the Student Database, and sharing of that information, is limited to Student Accounts staff and student employees, Financial Aid staff, and other staff specifically with a need to know.

Account information may be shared with outside agencies, usually those who contribute financially on behalf of the student, only when instructed by the student to do so and/or with documentation to do so.

Account information may be shared with outside agencies with a legitimate interest to know, such as University Affiliates, Wood Dining Service, the PA State Attorney General's office, collection agencies, university Legal Counsel, state or federal agencies on official business, law enforcement agencies, US Dept of Education, state or contracted auditors, or as a result of subpoenas or bankruptcy proceedings.

Perkins Loan Administration

The Perkins Loan Administrator follows all procedures outlined above. Student account information is shared directly with the Perkins Servicer, Educational Computer Services, Inc. (ECSI), on a secure network (see ECSI Information Security Plan and SU Information Systems Security Plan).

Perkins Service Provider (ECSI) and any Collection Agencies used by the university in collecting Perkins Loan funds must supply SU with copies of their safeguarding procedures (see appendix).

Account information may be shared with outside agencies included in *Account Information on Student Information System* above, and also with National Credit Bureaus.

Information Security Plan Academic Success Program 2004

Employee Management

Department Employees (Faculty, Staff, Graduate Assistants, Work-Study, and Interns)

New employees are briefed regarding security and confidentiality of information for employees, students, university employees, and family members. Policy and safeguarding of records reminders are reviewed during staff meetings and are part of the orientation for new graduate and work-study students. All graduate students, interns and work-study students are required to sign a confidentiality agreement, which also stipulates potential courses of action for a breach of the policy. New program students are required to sign a release of information form that allows ASP support staff and faculty members to share information in and between departments and supportive family members on their behalf. Students receiving supportive services through the Office of Social Equity must sign a release of information form, which provides the sharing of Individual Education Plans and any Educational Psychological Assessments that assist program faculty and staff to better meet the students' needs.

Physical Security

When not directly in use, all offices are locked. Access to these offices is limited by a single door for which keys are distributed only to the program secretary, Director, and the employee assigned to work in that office. The program secretary has a master key, which allows access to all offices and is only used in cases of emergency. Graduate assistants gain access to their offices via a master key that allows access to the common areas, such as the conference room and the copier room.

Phone Contacts

Information that is verified via the telephone includes current and past employers, students and parents' names, and classification. No information is released unless the student has approved the release of the information verbally and/or in writing. Information will only be mailed out when the employee, student, or other responsible party grants permission via a signed authorization form.

Computer Access

All Academic Success Program employees are given access to only those terminals and transactions that are necessary for the successful performance of their duties. Access to computer-based information is password protected. Computers in the common areas, such as the conference room and the copier room, allow for general use of such applications as Microsoft Word and Photo Deluxe.

Shredding Documents

The Academic Success Program has one location where documents are placed to be shredded. The location is away from visitors entering the collective office areas. All information that contains social security numbers is shredded after use.

Student Files/Records

There are three phases of the student record keeping process that are active within the Academic Success Program. These include: Current-Permanent files, Current-informal files, and Archival files.

Current-Permanent files: These files are the permanent official files that are required by the Department of Education. Included in these files are student eligibility information for the Act 101 grant such as high school transcripts, documentation of contact university correspondence, use of academic support services, university transcripts, and program specific correspondence for currently enrolled program students. These files are maintained and secured in locked file cabinets in the program office. Access to these files requires the key from the program secretary or the program director. Files are not permitted to leave the office, and the door is kept locked when the secretary, professional staff and/or the director is not present.

Current-Informal files: These files are maintained within the offices of the professional counselors, and the graduate assistants. Included in these files are documents such as contact logs, goal planning information, transcripts, parent contact information, correspondence from and to the students, and proposed scheduling information. All files are secured in a locked file cabinet or desk in each office. Those few offices that have not been equipped with locked cabinets are scheduled to receive locked cabinets within the next budget cycle. In the interim, office doors are locked when not in use. Access to these files requires the office key from the program faculty, program secretaries, or the program director.

Archival-Permanent files: These files contain information on former program students and include drop-outs, stop-outs and alumni. Files are secured in two places: the copier/supply room located in Wright Hall room 301 and the basement of Horton Hall, room #7. Information in Wright Hall 301 is kept in two file cabinets, however only one file cabinet has a locking mechanism. Files for the non-locked cabinet are secured via locking the door to the room itself. The files in Horton Hall are maintained in a secured closet within the room.

**SECURITY PROCEDURES
FOR
THE OFFICE OF SOCIAL EQUITY**

EMPLOYEES

Professional and student employees are verbally informed that matters pertaining to the functions of the Office of Social Equity are “Confidential”, and that the violation of confidentiality can result in termination of their employment. This includes complaints filed under the University’s Administrative Fact-finding Boards and complaints filed with external agencies. Students will sign a statement indicating that they have been informed of the confidential nature of the functions of the Office (copy attached).

OFFICE MANAGEMENT

Complaint Files:

Complaint files are kept in a filing cabinet and are not accessed by undergraduate student workers or graduate assistants. Access to the files is restricted to the Director, Staff Associate, and Temporary employee. The files are kept in the filing cabinet for two years, and then retired to the Social Equity Bin in the Basement of Old Main. The files are boxed, taped securely and marked “confidential”, and dated.

Search Files:

Recruitment files are kept in filing cabinets for one – two years before being retired to the Social Equity Bin in the Basement of Old Main. The files are boxed, taped securely and marked for identification and dated. Students have access to the files for the purpose of filing pertinent materials. The files can be destroyed after five years.

Phone contact:

When inquiries are received regarding a complaint, or status on an employment action, students do not discuss the query with the caller. The calls are referred to the Director, the Staff Associate, or Temporary employee, who determines the appropriate response.

Computer Access:

Employees have access to student information and the affirmative action data; and, the graduate assistant’s have limited access to the data.

**SHIPPENSBURG UNIVERSITY
SECURITY PROCEDURES
FOR
THE OFFICE OF DISABILITY SERVICES**

EMPLOYEES

Professional and student employees are verbally informed that matters pertaining to the functions of the Office of Disability Services are “Confidential” and that the violation of confidentiality can result in termination of their employment. This includes documentation supporting a student’s need for “reasonable” accommodations. Graduate Assistants, interns and undergraduate student employees sign a statement indicating that they have been informed of the confidential nature of the functions of the office (copy attached).

OFFICE MANAGEMENT

Student Files:

Student files are kept in locking file cabinets. A graduate assistant is assigned to assist the director with Accommodation Notification Forms to faculty and others who have a need to know. The graduate assistant has unlimited access to the files. Graduate interns from the Counseling Department perform follow up, monitoring and one-on-one contact with select students. The intern has limited access to the files. Undergraduate student workers do not have access to the files. The files are maintained for the sole purpose of meeting the “reasonable” accommodation needs of the students who have registered with the office. After five years the files are destroyed. The information does not become a part of the student’s official university file. The student receiving services has the right to review and/or close their file at anytime.

Shippensburg University
Dean of Students Office
Safeguarding Procedures
Gramm-Leach-Bliley Act

Employees Management

When hired, all employees in the Dean of Students Office are briefed on FERPA and privacy of rights of students by the Dean of Students or designee. These issues are also discussed at staff meetings and retreats. Publications of current court cases and FERPA debates are regularly shared with staff.

Student employees are also briefed on FERPA and privacy issues when hired. Students are required to sign the agreement that the Information Security Committee designed. FERPA and privacy issues are discussed at the mandatory student meeting held each semester. Any breach of this agreement results in the loss of employment and possible judicial action by the university.

Safeguards

Paper Documents and Student Files:

Students' files are kept in secure locations (filing cabinets or secure desks) with limited access. These are secure at night and the office is locked. Only full time employees have key access to the office. Student employees are permitted access to these files on a need to know basis.

Any paper documents with a student's Social Security Number, disciplinary or confidential information are shredded.

Phone Contact:

A student's record will not be discussed on the phone.

Service at the Counter:

The Dean of Student's Office requires identification before any information will be given to a student at the counter. Confidentiality is difficult in this office with so many customers at the counter at the same time. If a student is comfortable discussing their record at the counter, provisions can be made to have the discussion in a more private environment.

Credit Cards

The Office of the Dean of Students will not accept credit card information.

Computer Access

All employees of the Office of the Dean of Students are given access to only those transactions on the student mainframe necessary to perform their duties. Student database access is approved only for other employees who have a need to know. Access to the mainframe and online information is password protected.

April 12, 2004

End User License Agreement (EULA)/Software Download

Terms of Use/Disclaimer

PLEASE READ BEFORE YOU CONTINUE

Use of this website and/or links herein
constitute agreement to the Terms of Use/Disclaimer notice.

NO WARRANTIES: TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER SHIPPENSBURG UNIVERSITY ("SU"), NOR ANY PERSON, EITHER EXPRESSLY OR IMPLICITLY, WARRANTS ANY ASPECT OF THIS SOFTWARE, INCLUDING ANY OUTPUT OR RESULTS OF THIS SOFTWARE. THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY WARRANTY OF ANY TYPE OR NATURE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY THAT THIS SOFTWARE IS FREE FROM DEFECTS.

ASSUMPTION OF RISK: THE RISK OF ANY AND ALL LOSS, DAMAGE, OR UNSATISFACTORY PERFORMANCE OF THIS SOFTWARE RESTS WITH YOU AS THE USER. TO THE EXTENT PERMITTED BY LAW, NEITHER SU, NOR ANY PERSON EITHER EXPRESSLY OR IMPLICITLY, MAKES ANY REPRESENTATION OR WARRANTY REGARDING THE APPROPRIATENESS OF THE USE, OUTPUT, OR RESULTS OF THE USE OF THIS SOFTWARE IN TERMS OF ITS CORRECTNESS, ACCURACY, RELIABILITY, BEING CURRENT OR OTHERWISE. NOR DO THEY HAVE ANY OBLIGATION TO CORRECT ERRORS, MAKE CHANGES, SUPPORT THIS SOFTWARE, DISTRIBUTE UPDATES, OR PROVIDE NOTIFICATION OF ANY ERROR OR DEFECT, KNOWN OR UNKNOWN. IF YOU RELY UPON THIS SOFTWARE, YOU DO SO AT YOUR OWN RISK, AND YOU ASSUME THE RESPONSIBILITY FOR THE RESULTS. SHOULD THIS SOFTWARE PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL LOSSES, INCLUDING, BUT NOT LIMITED TO, ANY NECESSARY SERVICING, REPAIR OR CORRECTION OF ANY PROPERTY INVOLVED.

DISCLAIMER: IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, SHALL SU, OR ANY PERSON BE LIABLE FOR ANY LOSS, EXPENSE OR DAMAGE, OF ANY TYPE OR NATURE ARISING OUT OF THE USE OF, OR INABILITY TO USE THIS SOFTWARE, INCLUDING, BUT NOT LIMITED TO, CLAIMS, SUITS OR CAUSES OF ACTION INVOLVING ALLEGED INFRINGEMENT OF COPYRIGHTS, PATENTS, TRADEMARKS, TRADE SECRETS, OR UNFAIR COMPETITION.

INDEMNIFICATION: TO THE EXTENT PERMITTED BY LAW THROUGH THIS LICENSE, YOU, THE LICENSEE, AGREE TO INDEMNIFY AND HOLD HARMLESS SU, ITS OFFICIALS AND EMPLOYEES, AND ANY PERSON FROM AND AGAINST ALL CLAIMS, LIABILITIES, LOSSES, CAUSES OF ACTION, DAMAGES, JUDGMENTS, AND EXPENSES, INCLUDING THE REASONABLE COST OF ATTORNEYS FEES AND COURT COSTS, FOR INJURIES OR DAMAGES TO THE PERSON OR PROPERTY OF THIRD PARTIES, INCLUDING, WITHOUT LIMITATIONS, CONSEQUENTIAL DAMAGES AND ECONOMIC LOSSES, THAT ARISE OUT OF OR IN CONNECTION WITH YOUR USE, MODIFICATION, OR DISTRIBUTION OF THIS SOFTWARE, ITS OUTPUT, OR ANY ACCOMPANYING DOCUMENTATION

End User License Agreement (EULA)/User Registration

Shippensburg University ResNet Terms of Use and End User License Agreement

Use of ResNet services constitute agreement to the Terms of Use/User Agreement.

NO WARRANTIES: TO THE EXTENT PERMITTED BY APPLICABLE LAW, NEITHER SHIPPENSBURG UNIVERSITY ("SU"), NOR ANY PERSON, EITHER EXPRESSLY OR IMPLICITLY, WARRANTS ANY ASPECT OF THIS SERVICE, INCLUDING ANY OUTPUT OR RESULTS OF THIS SERVICE. THIS SERVICE IS BEING PROVIDED "AS IS", WITHOUT ANY WARRANTY OF ANY TYPE OR NATURE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ANY WARRANTY THAT THIS SERVICE IS FREE FROM DEFECTS.

ASSUMPTION OF RISK: THE RISK OF ANY AND ALL LOSS, DAMAGE, OR UNSATISFACTORY PERFORMANCE OF THIS SERVICE RESTS WITH YOU AS THE USER. TO THE EXTENT PERMITTED BY LAW, NEITHER SU, NOR ANY PERSON EITHER EXPRESSLY OR IMPLICITLY, MAKES ANY REPRESENTATION OR WARRANTY REGARDING THE APPROPRIATENESS OF THE USE, OUTPUT, OR RESULTS OF THE USE OF THIS SERVICE IN TERMS OF ITS RELIABILITY, AVAILABILITY, OR OTHERWISE. NOR DO THEY HAVE ANY OBLIGATION TO DISTRIBUTE UPDATES, OR PROVIDE NOTIFICATION OF ANY ERROR OR DEFECT, KNOWN OR UNKNOWN. IF YOU RELY UPON THIS SERVICE, YOU DO SO AT YOUR OWN RISK, AND YOU ASSUME THE RESPONSIBILITY FOR THE RESULTS. SHOULD THIS SERVICE PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL LOSSES, INCLUDING, BUT NOT LIMITED TO, ANY NECESSARY SERVICING, REPAIR OR CORRECTION OF ANY PROPERTY INVOLVED.

DISCLAIMER: IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, SHALL SU, OR ANY PERSON BE LIABLE FOR ANY LOSS, EXPENSE OR DAMAGE, OF ANY TYPE OR NATURE ARISING OUT OF THE USE OF, OR INABILITY TO USE THIS SERVICE, INCLUDING, BUT NOT LIMITED TO, CLAIMS, SUITS OR CAUSES OF ACTION INVOLVING ALLEGED INFRINGEMENT OF COPYRIGHTS, PATENTS, TRADEMARKS, TRADE SECRETS, OR UNFAIR COMPETITION.

INDEMNIFICATION: TO THE EXTENT PERMITTED BY LAW THROUGH THIS LICENSE, YOU, THE USER, AGREE TO INDEMNIFY AND HOLD HARMLESS SU, ITS OFFICIALS AND EMPLOYEES, AND ANY PERSON FROM AND AGAINST ALL CLAIMS, LIABILITIES, LOSSES, CAUSES OF ACTION, DAMAGES, JUDGMENTS, AND EXPENSES, INCLUDING THE REASONABLE COST OF ATTORNEYS FEES AND COURT COSTS, FOR INJURIES OR DAMAGES TO THE PERSON OR PROPERTY OF THIRD PARTIES, INCLUDING, WITHOUT LIMITATIONS, CONSEQUENTIAL DAMAGES AND ECONOMIC LOSSES, THAT ARISE OUT OF OR IN CONNECTION WITH YOUR USE, OF THIS SERVICE, ITS OUTPUT, OR ANY ACCOMPANYING DOCUMENTATION.

Terms and Conditions Specific to ResNet

User Responsibility:

The ResNet user is responsible for all use of their network connections. The ResNet user will be held accountable for any violations that occur involving their computer or network connections. Students should only allow others to use their machine with the full understanding of the consequences of that action. It is the responsibility of all users to maintain reasonable security and anti-virus protection for their systems. This includes using a secure administrator password, maintaining the latest operating system security updates, and regularly updating anti-virus protection with the most recent virus definitions. Systems found to be vulnerable to compromise, infected by a virus, or otherwise insecure, may be disconnected from the campus network until steps have been taken to secure and/or disinfect the system, as required.

Subscribers are responsible for all network usage associated with their computer and/or network connection. This includes all network traffic originating from off-campus for the purposes of connecting to or downloading from a computer, server, or other network device on ResNet (such as occurs with file-sharing).

In addition to the policies described in this document, as a user of university resources you are subject to applicable local, State, and Federal laws, as well as all relevant university and ResNet policies. Violations of this policy may be prosecuted under the guidelines set forth by Swatanev. Violations will be referred to the Dean of Students Office, or to the appropriate SU body adjudicating academic integrity, and/or to the appropriate local, State, and Federal authorities, as required. ResNet reserves the right to investigate suspected violations using all appropriate means. Furthermore, ResNet may terminate or restrict any person's access to its resources, without prior notice, if such action is necessary to maintain availability, security, and/or integrity of operations for other users of those resources. All users of university resources are expected to be familiar with and to abide by these regulations.

Anti-Virus Software:

ResNet users using Windows or Macintosh operating systems are required to use regularly updated anti-virus software on their computer(s). SU provides McAfee AntiVirus software free of charge to students, staff and faculty.

IP Address Usage:

ResNet subscribers are assigned an IP address for use with their specific computer or other networkable device. The use of any ResNet IP address other than that assigned by ResNet is prohibited. Subscribers who change jacks or rooms must update their subscription with ResNet (this can be done on-line) to receive their new IP address for that new location. Use of unassigned IP addresses can cause conflicts, possibly resulting in a disruption of service for the person assigned that address. ResNet subscribers are provided with one IP address for their primary computer or system.

Network Devices:

Any computer or other networkable device connected directly to the ResNet network must be registered with ResNet. The use of any unregistered device is prohibited. This includes, but is not limited to, game consoles, PDAs, printers, and any other networkable device. Subscribers can still use these devices, but they must be properly registered.

Use of network switching equipment such as hubs, switches, routers (wireless or otherwise), etc. is strictly prohibited. Only one Ethernet connection per user per data port is permitted. Use of network switching equipment for the purpose of network expansion, bridging, and/or multi-device access may result in your ResNet connection being suspended or terminated with or without prior notice.

Use of network devices in a "server" capacity is strictly prohibited. Use of such devices may result in your ResNet connection being suspended or terminated with or without prior notice.

Bandwidth Utilization:

SU sizes and acquires Internet bandwidth and network resources based on past usage statistics. While every effort is made to assure ample bandwidth is available to all campus network users, unexpected peak demand may cause degradation of services to all users until additional bandwidth is installed. To manage the impact at these times, traffic may be prioritized to assure critical communications are not adversely impacted.

Scanning & Network Security:

SU collects network usage statistics about all direct connections between SU/ResNet computers and external addresses (the Internet). This data is similar to the data collected for telephone connections: it consists of the information required to transfer the data (IP addresses, protocols, port numbers, and other routing information), the number of packets and bytes transferred, as well as a time stamp. SU reserves the right to conduct regular security scans of ResNet LANs to check for vulnerabilities, Trojan software, or other system compromises which could be exploited by other users.

All computers and networkable devices connected to ResNet will also be subjected to an initial security scan after subscribing to the service. Any systems found to be insecure or otherwise vulnerable to compromise may be refused access, disconnected from the campus network, or have access restricted until such time as the user takes the necessary steps to secure their system.

General Usage:

University owned computers and networks are governed by policies and codes as well as federal, state, and local laws. In addition, all non-university computers and servers using these networks are

governed by the same policies. Among other restrictions, the operation of any commercial or for-profit enterprise or advertising is prohibited, along with any re-sale of access or services. Illegal activities -- including, but not limited to, such practices as fraud, harassment, software piracy, and copyright infringement -- are, of course, also prohibited. In addition, IP spoofing, packet sniffing, virus distribution, or any activity that disrupts the network are violations of SU computer abuse policies. The university reserves the right to place limited restrictions on the use of its computers and network systems in response to complaints presenting evidence of violations of university policies or codes, or state or federal laws. Once evidence is established, computers involved in alleged violations may be disconnected from the network until the situation is resolved. ResNet allows access to the University mainframe computer, library resources, e-mail, and the Internet (which includes the World Wide Web). ResNet is designed and maintained for academic use only. ResNet does not specifically bar use of network resources for additional, legal uses (such as gaming), but neither supports nor devotes network resources for such activities.

Correspondence from ResNet:

ResNet users will receive occasional correspondence from ResNet staff. By agreeing to the terms and conditions for service, you agree to receive this information.

Service Interruptions:

Network service may be interrupted on occasion. ResNet will work to restore service as soon as practicable; however, SU and ResNet are not responsible for any losses or damages caused by service interruptions or other failures in University equipment.

Statement on Peer-To-Peer (File Sharing/"P2P") Applications and Use:

ResNet does not specifically bar the installation or use of P2P applications. We do not, however, support or devote resources to such applications. Use of these applications is at the user's own risk. Use of P2P applications for the purpose of "serving" content is prohibited, as this constitutes the use of your computer or networkable device in a server capacity. Any use of P2P or similar applications for the purpose of serving or trafficking protected content (i.e. copyrighted materials) may result in the suspension or termination of service without prior notice. All notices of such activity or alleged activity presented to the ResNet office will be investigated and referred to the appropriate adjudicating body in accordance to the terms set forth in this agreement.

Statement on Gaming Software:

ResNet does not specifically bar the installation or use of computer games or software used to connect to gaming platforms and/or gaming servers. We do not, however, support or devote resources to such applications. Use of these applications is at the user's own risk.

Change of Terms of Use and End User License Agreement ("EULA"):

This Terms of Use and EULA is subject to change without notice. ResNet may also make improvements and/or changes in the services described in this agreement at any time without notice. The terms and conditions contained in this legal notice are subject to change without notice, and you should visit the ResNet website periodically to determine if any such changes have been made.



Shippensburg University • Etter Health Center
 71 Old Main Drive • Shippensburg, Pennsylvania 17257 • (717) 477-1458
 • FAX (717) 477-4042 •

Johnson G. Coyle, M.D., Medical Director

**AUTHORIZATION FOR RELEASE OF INFORMATION
 TO PARENT(S) OR GUARDIAN(S)**

I, _____, authorize release of medical formation
PRINT Student Name

Records To:

Social Security Number

Date of Birth

Name _____
 Address _____
 Phone _____
 Fax _____

Records From:

ETTER HEALTH CENTER

1871 Old Main Dr.

Shippensburg, PA 17257

Name _____
 Address _____
 Phone _____
 Fax _____

Fax #: (717) 477-4042

Name _____
 Address _____
 Phone _____
 Fax _____

Include Disclosure of Records For:

<u>Yes</u>	<u>No</u>	Reproductive Health	<u>Yes</u>	<u>No</u>	Drug/Alcohol Treatment
___	___	AIDS/HIV	___	___	Psychiatric/Mental Health

GENERAL AUTHORIZATION: I understand and acknowledge that this authorization allows the health care facility to release all or part of the records indicated above to my parent or guardian. I understand that, on occasion, information may be released by telephone or fax.

This consent is valid for academic year ___ - ___, unless revoked by me in writing before the release of the above-designated information.

I read this form, or had it read to me and I understand it. I was given an opportunity to ask questions. Any question I asked was answered to my satisfaction. My signature below indicates my voluntary authorization for the release of information.

Signature of Student **Date** _____
Signature of Witness **Date**

****NOTICE****

Please allow 48 hours for processing a routine request. All emergency requests from your physician will be given the appropriate attention. Thank you for your cooperation in this matter.



Etter Health Center

Shippensburg University • Etter Health

1871 Old Main Drive -Shippensburg, Pennsylvania 17257- (717) 477-1458 –
FAX (717) 477-404

Johnson G. Coyle, M.D., Medical Director

AUTHORIZATION FOR RELEASE OF INFORMATION

I,

Patient Name: **PRINT**

Social Security Number

authorize release or medical

Date of Birth

Records From:

Records To:

Fax #:

Fax#:

**Date of Treatment:
Records to Include:**

- Initial H&P
- Labs/X-ray
- Closing Summary

Include Disclosure of Records For:

- | <u>YES</u> | <u>NO</u> | |
|--------------------------|--------------------------|--|
| <input type="checkbox"/> | <input type="checkbox"/> | <i>Drug/ Alcohol Treatment</i> |
| <input type="checkbox"/> | <input type="checkbox"/> | <i>AIDS/HIV</i> |
| <input type="checkbox"/> | <input type="checkbox"/> | <i>Psychiatric/Mental Health
(If 3yes, include the Special
Authorization Form)</i> |

GENERAL AUTHORIZATION: I understand and acknowledge that this general authorization allows the health care facility to release all or part of the records indicated above for the purpose stated. I understand that, on occasion, information may be released by telephone or fax.

This consent is valid for 90 days, unless revoked by me in writing before the release of the above designated information.

I read this form, or had it read to me and I understand it. I was given an opportunity to ask questions. Any question I asked was answered to my satisfaction. My signature below indicates my voluntary authorization for both the general and special release of information.

Signature of Patient

Date

Signature of Witness

Date

****NOTICE****

Please allow 48 hours for processing a routine request. All emergency requests from your physician will be given the appropriate attention. Thank you for your cooperation in this matter.

AUDIO/VIDEO TAPE RELEASE FORM

The University Counseling Center is actively involved in training and supervision. We believe that this can best be facilitated by observation and/or taping of counseling sessions; this provides feedback to counselors and allows the services provided to you to be more effective.

I understand that training is a function of the University Counseling Center and give permission for (check the following that apply):

_____ audio-taping of counseling sessions

_____ video-taping of counseling sessions

_____ observation of counseling sessions

I understand that all information about counseling sessions is confidential and that all recorded information is used only for training purposes. I have also been given the opportunity to ask questions concerning these observations and am satisfied that my questions have been answered.

(Client's Signature) (Date)

(Client's Signature) (Date)

Group Member / Leader Confidentiality Statement

As a participant of this group, I realize that it the responsibility of myself and all other group participants to keep the group confidential. This means that I am not free to share with others who are not currently group participants the names of group members, and what is discussed in the group. This does not stop me from sharing with others the fact that I am in the group as long as I do not violate the above. It is the responsibility of the group leaders to keep all records confidential.

I have read, understood and agree to the information on this sheet.

Signature

Date

Group Name: _____

Semester: _____

Facilitator(s): _____

**Shippensburg University
Department of Public Safety
Safeguarding Procedures**

Employee Management

Department Employees

- New employees are briefed regarding security and confidentiality of all issues, records, or information discussed or disseminated within the department.
- Related issues are discussed regularly at supervisor and departmental meetings.

Student Employees

- Student employees in the Department of Public Safety are required to sign a confidentiality agreement.
- The student supervisor will discuss the importance of confidentiality and the consequences of a breach of agreement with the student.

Office Safeguards

Paper Documents and Files in Office

- Police complaint and incident reports as well as any other confidential documents are stored in filing cabinets within the department as well as electronically on department computers. Access to these documents is restricted to departmental personnel only and is password protected. The police department area is staffed at all times so control of documents is maintained.
- Any reports kept by officers for court or other purposes are stored in locked file drawers with each officer having a key to his or her drawer only.
- Juvenile records / reports are stored in a separate secure area.
- Any information released to other police departments for investigative purposes is documented and filed.
- Reports received or produced by the Safety Coordinator or his / her clerk, are stored in the Safety office. When not staffed, this office is kept locked at all times.
- Any paper document containing confidential information that is no longer needed is shredded by department personnel.

Paper Documents and Files in Archives

- Archived files are placed in boxes and stored in a locked area in the lower level of the department. Access to this area is restricted to departmental personnel only.
- Records or files that are purged are shredded before disposal.
- Records produced by the police department are kept in secure storage for a minimum of 10 years before being destroyed.
- Records produced by the Safety Coordinator or his / her clerk are kept in secure storage for a minimum of 20 years before being destroyed.

Phone Contact

- Departmental information will not be discussed on the phone unless proper identification is provided by the caller.

Service at the Front Desk

- Departmental information will not be discussed at the front desk unless proper identification is provided by the subject requesting information.

Computer Access

- Access to Mainframe, and online information is password protected.
- Employees of the Department of Public Safety are given access to Mainframe necessary to perform their duties.
- Student use of Mainframe is limited and access is provided by their supervisor on an as needed basis.

Shippensburg University
Human Resources Department
Confidential Information Safeguarding Procedures

Employee Management

Department Employees

1. New employees are briefed regarding security and confidentiality of information for employees, students and applicants.
2. Related issues are discussed regularly at staff meetings and weekly meetings with the Director.
3. Publications with related articles/information are shared with staff members.

Interns

1. Student interns are briefed regarding security and confidentiality of information for employees, students and applicants.
2. Student interns must sign a confidentiality statement, a breach of which could result in loss of the intern opportunity.
3. Related issues are discussed regularly throughout the intern experience. Publications with related articles/information are shared with the intern.

Office Safeguards

Paper Documents and Files in Office

1. Confidential documents are stored in cabinets/drawers in each individual office.
2. Paychecks are sealed prior to delivery to the office and are kept in file cabinets which can only be accessed by office employees. This file room is locked during non-work hours.
3. The office is kept locked during non-work hours. Only office employees and essential University employees have key access.
4. Any paper document with an employee or student SSN or other confidential information that is no longer needed is shredded.
5. Personnel files are stored in a file closet and are accessible by office members only. This file room is locked during non-work hours.
6. Employee Benefit files are stored in a file cabinet separate from the personnel files. This file cabinet is locked during non-work hours.
7. The SSN is removed or not listed on forms that do not actually require it's presence. The Employee Tuition Waiver forms have been modified so that we will not require the students' Social Security numbers and instead ask for the Student ID numbers.

Paper Documents and Files in Archives

1. Archived files are locked in a separate storage space which can only be accessed by office members.
2. Records or files that are purged are shredded before disposal. The following schedule is followed for retention and disposition:
 - a. Payroll records—shredded after seven years
 - b. Job Description—current copy kept on file, older versions shredded
 - c. Time and Attendance Records—shredded after five years
 - d. Worker's Compensation records—shredded after thirty years
 - e. Search Applications—shredded after three years
 - f. Unsolicited Employment Applications—shredded after six months

Personnel File Access

1. Individuals who request access to a personnel file will be briefed regarding security and confidentiality of information prior to reviewing the file. Files that they may review

include an employee under their direction, an internal candidate for an open position in their department, or an individual whose file will be reviewed regarding official union business. Under no circumstances will the file be removed from the office and review of the contents will be in the presence of a Human Resources Department staff member.

2. Only pertinent sections of the file will be made available to the person reviewing the materials (i.e. performance evaluations, training records, attendance records etc.)
3. Requests for copies of previous performance evaluations and job descriptions will be granted to supervisors, but social security numbers will be removed prior to the copies being forwarded.

Phone Contact

1. Information verified via the telephone includes employee name, classification, and dates of employment. Any other requests for information must be submitted in writing and would only be released with a signed authorization from the employee or other responsible party.

Employee Service

1. Employees with benefit questions are asked to write their SSN on a piece of paper instead of stating it out loud if they are being assisted in a common area of the office. Those who are receiving assistance in an office do not need to write the SSN down if the door is closed during the meeting.

Computer Access

1. All Human Resources employees are given access to only those transactions necessary to perform their duties.
2. Access to computer-based information is password protected.
3. Computer screens are turned so that customers may not view what is being accessed on the screen.

revised and approved by President's Cabinet: 7/07

Communication/Education Plan

Safeguarding of Customer Information

Target Audience—*Any University personnel who have access to a system that has customer information, access to paper copies of customer information or supervises these individuals.*

Information to be covered:

- Background—GLB Act, FERPA, HIPAA, who these affect, why they are important etc.
- Ship's policy
- Who are the customers, who handles this information
- What kind of information is to be safeguarded
- Physical procedures—locking cabinets, shredding documents, etc.
- Practices—writing down SS numbers, accounts numbers instead of saying them etc.
- Who to contact with questions (what should be shredded, availability of a central shredder, etc.)

Initial Education

1. General overview offered to campus community (possibly different sessions targeting faculty, staff and administration)
2. Roll-out communication through Vice Presidents, Deans Directors via existing channels (committees, staff meetings, Dean's Council etc.)
3. FACT/HR Update coverage

On-going Education

1. General orientation offered by Human Resources (handout/brochure covering basics)
2. Basic confidentiality agreement signed by new employees during benefits overview in Human Resources
3. Faculty orientation coverage
4. Department specific orientation—specifics for particular area addressed, confidentiality agreement signed)
5. FACT/HR Update
6. Covered annually with other policies—Drug Free Workplace, Sexual Harassment etc.
7. Coverage at University web site—possibly a virtual orientation or a tutorial

FERPA Actions Currently in Place Registrar's Office

There is a FERPA statement on the Registrar's Office website at <http://www.ship.edu/admin/registrar/ferpa.html>.

The Office of the Registrar has arranged for statements to be placed on the following areas explaining the responsibilities of the user in viewing any of the information:

- a. Student Mainframe
- b. Department Information Systems (online service for departments)
- c. Faculty Information Systems (online service for faculty)

At the end of Spring 2004, the Registrar has conducted the following workshops on FERPA:

- a. Four advisor workshops (Advisor Development Program)
- b. Two other workshops during the 2003-2004 academic year (Dean of Students staff and Council of Education and Human Services).
- c. Mini-session to bring the Admissions Office staff up-to-date
- d. Meets with staff and deans' administrative assistants monthly and often reviews FERPA issues.

At the beginning of each semester, class lists are distributed to each faculty member and with the class lists is a briefing on FERPA for faculty (copy attached). FERPA guidelines are also distributed with materials to new faculty during orientation.

Once per year, students are sent a briefing of their Right-to-Know laws (copy attached).

Alana Moriarty
February 17, 2004

Confidentiality Statements and Training

Beginning immediately and as part of the process of administering the completion of payroll documents, Human Resources will ask all new employees and all new student workers to read and sign the general confidentiality statement as identified in the Information Security Plan. Departments and offices may supplement this with their own unique policies and statements.

rev. 10/31/06

adopted by President's Cabinet: __/__/06

Student Employee Confidentiality Agreement

I acknowledge that as a student employee/graduate assistant of Shippensburg University, I may have access to confidential information and records for which unauthorized disclosure is strictly prohibited.

I further understand that unauthorized disclosure of confidential information and records applies to all information in university files, discussed in the office or on the telephone and on the university computing/networking systems.

I recognize that if I fail to uphold this standard of confidentiality it will result in the termination of my position as well as possible university judicial action against me.

Having read this Student Employee Confidentiality Contract, I agree that I will not access confidential information, nor will I disclose confidential information to others, except as required by my job duties.

I have had the opportunity to discuss this responsibility with my supervisor and he/she has addressed any questions or concerns I have voiced.

Student's Name _____ SSN _____

Student's Signature _____ Date _____

I have discussed the confidentiality aspect of this position with the above named student employee/graduate assistant and he/she has acknowledged their understanding and acceptance of the above.

Supervisor's Signature _____ Date _____

Pennsylvania State System of Higher Education Confidentiality Statement

Background

With the implementation of the Shared Administrative System Human Resource/Payroll module using SAP technology, more information will be stored in electronic format. It is essential that the confidentiality and privacy of this information be maintained. As a Pennsylvania State System of Higher Education (System) employee who has been given access to confidential information, it is your responsibility to protect this sensitive and personal data.

System management and employees are relying on you to maintain confidentiality of the employee data and to access, use, discuss, release, and disclose this data only when it is dictated by your job duties. If you do not need to access employee information to perform your job, under no circumstances should it be accessed. If you do need to access employee information to perform your job, the information should not be divulged to anyone unless it is done so through authorized protocols.

To ensure that all System employees with access to SAP Human Resource/Payroll System information are aware of this confidentiality requirement, you must sign and date the statement below. You should retain a copy of this notice for your records and return the original copy of this form to your human resource office. If you have any questions regarding your responsibility to maintain confidentiality of the data to which you have access in your work associated with the SAP Human Resource/Payroll system, you should contact your human resource director.

Confidentially Statement

As an employee of the Pennsylvania State System of Higher Education (System), I understand that I may have access to confidential, personal data of System employees. I agree that I will access, use, discuss, release, and/or divulge only the data that is needed to perform my job. I understand that I am prohibited from accessing, using, discussing, releasing, and/or divulging this data unless doing so is a requirement of my job. I understand that any release of this information will be done only through authorized protocols. For System employees, breaches in confidentiality of such data may result in disciplinary action up to and including separation from employment. A violation of this agreement also may result in criminal action if it is determined that any local, state, or federal law has been violated.

By my signature below, I am certifying that I have read, understand, and agree to abide by the provisions of this policy.

Signature

Date

Print Name

University

Shippensburg University
Purchasing & Contracting Office
Information Security Plan
Gramm-Leach-Bliley Act

Office Safeguards

Contract documents and purchase orders that may contain contractor's social security numbers are kept in filing cabinets and have limited access. The offices are locked at night. Only full time employees have key access to the offices.

Retired files are stored in the Old Main basement in a locked room with limited key access and kept for three years. After 3 years, all documents will be shredded.

Service Provider Contracts

Where the University has contracted with third parties for services, and those Contractors have access to relevant financial data, the contracts will include the following amendment language to contractually require the service providers to implement and maintain safeguards.

When issuing new contracts for services, the University will take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for customer information and the service providers will be contractually bound by the contract language to implement and maintain such safeguards.

SHIPPENSBURG UNIVERSITY CONFIDENTIAL INFORMATION ADDENDUM

This Addendum ("Addendum") amends and is hereby incorporated into the existing agreement known as _____ ("Agreement"), entered into by and between _____ (hereinafter "Service Provider") and Shippensburg University on _____.

Shippensburg University and Service Provider mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Gramm Leach Bliley Act ("GLB") dealing with the confidentiality of customer information and the Safeguards Rule. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:

a. *Covered Data and Information* includes *Student Financial Information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

b. *Student Financial Information* is that information that the university has obtained from a customer in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 C.F.R. § 225.28. Examples of student financial information include

addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information. Specifically, access to the following categories of Covered Data and Information is anticipated under the Agreement:

3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the covered data and information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of Shippensburg University except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by Shippensburg University.

4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of Shippensburg University according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:

a. Return to Shippensburg University or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of Shippensburg University. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to Shippensburg University that such return or destruction has been completed.

b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Service Provider shall extend the protections of this Addendum to Covered Data and Information received from or created on behalf of Shippensburg University, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.

6. Term and Termination:

- a. This Addendum shall take effect [upon execution].
- b. In addition to the rights of the parties established by the underlying Agreement, if Shippensburg University reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Addendum, Shippensburg University, in its sole discretion, shall have the right to:
 - (i) exercise any of its rights to reports, access and inspection under this Addendum; and/or

- (ii) require Service Provider to submit to a plan of monitoring and reporting, as Shippensburg University may determine necessary to maintain compliance with this Addendum; and/or
 - (iii) provide Service Provider with a fifteen (15) day period to cure the breach; and/or
 - (iv) terminate the Agreement immediately if Service Provider has breached a material term of this Addendum and cure is not possible.
 - c. Before exercising any of these options, Shippensburg University shall provide written notice to Service Provider describing the violation and the action it intends to take.
7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, Shippensburg University to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Addendum.
 8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, Shippensburg University.
 9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall report to Shippensburg University any use or disclosure of Covered Data and Information not authorized by this Addendum or in writing by Shippensburg University. Service Provider shall make the report to Shippensburg University not less than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Covered Data and Information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service Provider shall provide such other information, including a written report, as reasonably requested by Shippensburg University.
 10. Indemnity. Service Provider shall defend and hold Shippensburg University harmless from all claims, liabilities, damages, or judgments involving a third party, including Shippensburg University's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Addendum.
 11. Survival. The respective rights and obligations of Service Provider under Section 5 shall survive the termination of this Agreement.

Surplus Disposal Sale

The University issues public notice of items that are surplus to its needs, to be sold by sealed bid. The University Information Technologies and Services Office is responsible to clear all the data from any surplus computers, prior to them being offered for sale to the public.

March 24,2004

SHIPPENSBURG UNIVERSITY CONFIDENTIAL INFORMATION ADDENDUM

This Addendum (“Addendum”) amends and is hereby incorporated into the existing agreement known as _____ (“Agreement”), entered into by and between _____ (hereinafter “Service Provider”) and Shippensburg University on _____.

Shippensburg University and Service Provider mutually agree to modify the Agreement to incorporate the terms of this Addendum to comply with the requirements of the Gramm Leach Bliley Act (“GLB”) dealing with the confidentiality of customer information and the Safeguards Rule. If any conflict exists between the terms of the original Agreement and this Addendum, the terms of this Addendum shall govern.

1. Definitions:

a. *Covered Data and Information* includes *Student Financial Information* (defined below) required to be protected under the Gramm Leach Bliley Act (GLB), as well as any credit card information received in the course of business by the University, whether or not such credit card information is covered by GLB. Covered data and information includes both paper and electronic records.

b. *Student Financial Information* is that information that the university has obtained from a customer in the process of offering a financial product or service, or such information provided to the university by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student’s parent when offering a financial aid package, and other miscellaneous financial services as defined in 12 C.F.R. § 225.28. Examples of student financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers, in both paper and electronic format.

2. Acknowledgment of Access to Covered Data and Information: Service Provider acknowledges that the Agreement allows the Service Provider access to Covered Data and Information. Specifically, access to the following categories of Covered Data and Information is anticipated under the Agreement:

3. Prohibition on Unauthorized Use or Disclosure of Covered Data and Information: Service Provider agrees to hold the covered data and information in strict confidence. Service Provider shall not use or disclose Covered Data and Information received from or on behalf of SHIPPENSBURG University except as permitted or required by the Agreement or this Addendum, as required by law, or as otherwise authorized in writing by SHIPPENSBURG University.

4. Safeguard Standard: Service Provider agrees that it will protect the Covered Data and Information it receives from or on behalf of SHIPPENSBURG according to commercially acceptable standards and no less rigorously than it protects its own confidential information.

5. Return or Destruction of Covered Data and Information: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall:

a. Return to SHIPPENSBURG University or, if return is not feasible, destroy all Covered Data and Information in whatever form or medium that Service Provider received from or created on behalf of SHIPPENSBURG University. This provision shall also apply to all Covered Data and Information that is in the possession of subcontractors or agents of Service Provider. In such case, Service Provider shall retain no copies of such information, including any compilations derived from and allowing identification of Covered Data and Information. Service Provider shall complete such return or destruction as promptly as possible, but not less than thirty (30) days after the effective date of the conclusion of this Agreement. Within such thirty (30) day period, Service Provider shall certify in writing to SHIPPENSBURG University that such return or destruction has been completed.

b. If Service Provider believes that the return or destruction of Covered Data and Information is not feasible, Service Provider shall provide written notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction is not feasible, Service Provider shall extend the protections of this Addendum to Covered Data and Information received from or created on behalf of SHIPPENSBURG University, and limit further uses and disclosures of such Covered Data and Information, for so long as Service Provider maintains the Covered Data and Information.

6. Term and Termination:

a. This Addendum shall take effect [upon execution] [May 23, 2003].

b. In addition to the rights of the parties established by the underlying Agreement, if SHIPPENSBURG University reasonably determines in good faith that Service Provider has materially breached any of its obligations under this Addendum, SHIPPENSBURG University, in its sole discretion, shall have the right to:

(i) exercise any of its rights to reports, access and inspection under this Addendum; and/or

(ii) require Service Provider to submit to a plan of monitoring and reporting, as SHIPPENSBURG University may determine necessary to maintain compliance with this Addendum; and/or

(iii) provide Service Provider with a fifteen (15) day period to cure the breach; and/or

(iv) terminate the Agreement immediately if Service Provider has breached a material term of this Addendum and cure is not possible.

c. Before exercising any of these options, SHIPPENSBURG University shall provide written notice to Service Provider describing the violation and the action it intends to take.

7. Subcontractors and Agents: If Service Provider provides any Covered Data and Information which was received from, or created for, SHIPPENSBURG University to a subcontractor or agent, then Service Provider shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Service Provider by this Addendum.

8. Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted Covered Data and Information received from, or on behalf of, SHIPPENSBURG University.

9. Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information : Service Provider shall report to SHIPPENSBURG University any use or disclosure of Covered Data and Information not authorized by this Addendum or in writing by

SHIPPENSBURG University. Service Provider shall make the report to SHIPPENSBURG University not less than one (1) business day after Service Provider learns of such use or disclosure. Service Provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Covered Data and Information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service Provider shall provide such other information, including a written report, as reasonably requested by SHIPPENSBURG University.

10. Indemnity. Service Provider shall defend and hold SHIPPENSBURG University harmless from all claims, liabilities, damages, or judgments involving a third party, including SHIPPENSBURG University's costs and attorney fees, which arise as a result of Service Provider's failure to meet any of its obligations under this Addendum.

11. Survival. The respective rights and obligations of Service Provider under Section 5 shall survive the termination of this Agreement

IN WITNESS WHEREOF, each of the undersigned has caused this Addendum to be duly executed in its name and on its behalf.

FOR THE CONTRACTOR:

FOR THE UNIVERSITY:

Individual or Partner (if Contractor
is an individual or partnership)

Vice President of Administration & Finance

President or Vice President of
Corporate Contractor (circle title)

Fiscal Officer

Approved as to Form and Legality:

Secretary or Treasurer of
Corporate Contractor (circle title)

University Legal Counsel
State System of Higher Education

Deputy Attorney General

Note regarding signatures above. If a corporation, two signatures are required, one being the President or Vice President, the second being the Secretary or Treasurer. Signatory authority of either signatures can be delegated provided there is a certified Board resolution presented with this contract.

Last Revised 1-August-2007



Student information submitted by Clearinghouse Participants to the Clearinghouse is proprietary data and shall be used only for the purposes stated within the Participant's agreement with the Clearinghouse. The Clearinghouse has instituted reasonable controls to ensure that information it receives from Participants will be used only in accordance with applicable agreements and will be shared only with parties authorized to such information under applicable participant agreements or by law. Furthermore, the Clearinghouse has in place an information security program for protecting Participant's proprietary student information that fulfills the objectives set forth in the "Interagency Guidelines Establishing Standards for Safeguarding Customer Information", 66 Fed. Reg. 8616, February 1, 2001, (codified in Appendix B to 12 C.F.R. part 30.)

The Clearinghouse's security program, in accordance with the aforementioned regulation, is designed to (i) ensure the security and confidentiality of any Customer Information provided to the Clearinghouse, (ii) protect against any anticipated threats or hazards to the security or integrity of Customer Information, and (iii) prevent unauthorized access to or use of Customer Information. Participants will also institute reasonable controls to ensure that information it receives from the Clearinghouse will only be used in connection with its obligations under its applicable agreement with the Clearinghouse and shall be shared only with persons authorized to such information under applicable participant agreements or by law.

Regarding Gramm-Leach-Bliley (GLB)

To the extent that a Financial Institution Participant shares any of its Customer Information with the Clearinghouse, the Clearinghouse recognizes that it is subject to the reuse and redisclosure limitations of the Joint Banking Agencies' regulations implementing Title V of the Gramm-Leach-Bliley Act, Public Law 106-102 (the "GLB Requirements") and as such is prohibited from disclosing or using any such Customer Information except (i) as necessary to carry out the purposes for which the information was disclosed or (ii) as may be otherwise be permitted under an exception contained in Section 216.14 or 216.15 or Section 313.14 or 313.15, as applicable, under the GLB Requirements in the ordinary course of business to carry out the purposes for which the information was disclosed.

Copyright (c) 2004 by National Student Clearinghouse. All Rights Reserved [Terms of Use](#) | [Privacy Policy](#) | web-master@studentclearinghouse.org

Procedure for Responding to Right-to-Know Requests for Shippensburg University of Pennsylvania

A. Requests

- 1) Requests for information under the Right-to-Know Law must be submitted in writing to the designated right-to-know officer. A request may be delivered in person or via letter, facsimile, or electronic mail. Shippensburg University will not respond to oral requests.
- 2) Shippensburg University will not respond to anonymous requests for information.
- 3) In accordance with the Act, Shippensburg University will provide a requester with access to a public record only if the requester is an individual who is a resident of Pennsylvania. The Act does not require an agency to respond to requests from corporations, even if the corporation was created under the laws of Pennsylvania.
- 4) Each request must include the name of the requester and the address to which the response will be delivered. The request should identify or describe the records sought with sufficient specificity to enable Shippensburg University to ascertain which records are being requested.
- 5) The right-to-know officer may ask the requester the reason for the request or the intended use of the records in order to help identify the records of actual relevance to the requester. Shippensburg University cannot insist that such a statement be provided, nor can it use the lack of such a statement as a reason for denying the request.

B. Submittal of Right-to-Know Requests

- 1) All requests to Shippensburg University under the Right-to-Know Law will be submitted in writing to:

Dr. Peter M. Gigliotti
Executive Director for University Communications and Marketing
306 Old Main
Shippensburg University
1871 Old Main Drive
Shippensburg, PA 17257-2299

Approved by President's Cabinet 3/15/04

Requests may be delivered in person to the address listed above or sent by regular mail. They also may be submitted via facsimile to: (717) 477-4079 or via electronic mail to: pmgigl@ship.edu.

- 2) If a request is delivered to someone other than the right-to-know officer, it shall be forwarded to the right-to-know officer in a reasonable time. The 10- business-day period for a response to the request begins once the designated right- to-know officer receives the request.
- 3) The right-to-know officer will inform the requester of receipt of the request, including the date the request was deemed received.

C. Shippensburg University's Duty to Provide a Prompt Response to a Right-to- Know Request

- 1) Upon receipt of a written request; Shippensburg University will make a good faith effort to determine if the requested record is a public record and to respond as promptly as possible under the circumstances existing at the time of the request. This time shall not exceed 10 business days from the date the written request is received by the right-to-know officer. If Shippensburg University fails to respond within that time period, the request is deemed denied.
- 2) Shippensburg University may inform the requester of the need for additional time to comply with a specific request, in accordance with provisions of the Act. Such an extension may not exceed 30 calendar days. In such cases, if Shippensburg University fails to make a timely final response, the request is deemed denied.

The right-to-know officer shall send written notice to the requester within ten business days of the need for an extension. The notice shall include a statement notifying the requester that the request for access is being reviewed, the reason for the review and a reasonable date that a response is expected to be provided.

D. Processing of Right-to-Know Requests

- 1) Upon receiving a written Right-to-Know request, the right-to-know officer shall complete the following tasks:
 - a) Date-stamp the request.
 - b) Assign a tracking number to the request.
 - c) Compute the day on which the 10-business-day period will expire and make a notation of that date on the first page of the request.

- d) Inform the requester of receipt of the request.
 - e) Make an electronic or paper copy of the request, including all documents submitted with it and the envelope (if any) in which it came.
 - f) Create an official file for the retention of the original request.
- 2) For purposes of determining the 10-business-day period:
- a) A business day shall be any Monday, Tuesday, Wednesday, Thursday, or Friday, except those days when the offices of the agency are closed for all or part of a day due to a state holiday, due to severe weather (such as a blizzard or ice storm); due to natural or other disaster; or due to the request or direction of local, state, or federal law enforcement agencies or officials.
 - b) Requests may be submitted during regular business hours, which are 8 a.m. to 4:30 p.m. Requests received after 4:30 p.m. will be deemed to have been received on the following business day.
 - c) For purposes of determining the end of the 10-business-day period, the day that a request is received (or deemed to be received) is not counted: The first day of the 10-business-day period is the agency's next business day.

E. Initial Review by the Right-to-Know Official

- 1) Upon receiving a right-to-know request, the right-to-know official shall promptly review it. The purpose of this review is to determine the following:
 - a. Whether the request possesses an obvious defect that permits it to be rejected without further consideration. Such defects include the following.
 - 1) The face of the request unambiguously establishes that the requester is not a resident of Pennsylvania.
 - 2) The documents sought by the requester are not identified with sufficient particularity.
 - 3) The identified records unquestionably fall outside either of the two parts of the Act's general definition of "public records."
 - 4) The identified records unquestionably fall within one of the Act's statutory exemptions to the definition of "public records."
 - 5) The right-to-know official has personal knowledge that the identified records do not exist.
 - 6) The right-to-know official has personal knowledge that the identified records are not in the possession or control of the agency.

- b. Whether the request can be granted without further consideration. For example, if the right-to-know official is satisfied that the requester is a resident of Pennsylvania, and knows that the requested documents exist and are public records and that they are immediately accessible, no further analysis is necessary.
 - c. Whether the request implicates a right protected by the Pennsylvania or U.S. Constitution, including but not limited to, the constitutional right of privacy. If the right-to-know official concludes that the request implicates such a right, he shall consult with counsel regarding the balancing of the requester's interest in access to the records versus the constitutionally protected interests.
- 2) In conducting this initial review, the right-to-know official may contact (or attempt to contact) the requester in order to obtain clarification or additional information.
- 3) If the right-to-know official determines that the request should be refused for any of the grounds set forth in (1), above, he shall immediately draft a proposed refusal letter. This draft should set forth each and every ground that the right-to-know official believes is a proper ground for refusal.

F. Responses, In General

- 1) The act of providing a requester with physical access to a document in the offices of the agency is a "response" for purposes of the Right-to-Know Act.
- 2) A record will be provided, whenever available, in the medium requested by the requester (i.e., an electronic file if the information is already available in this form.). A record does not have to be converted to a media other than that in which it is maintained.
- 3) A requester may either view original records by making an appointment during regular business hours with the right-to-know official, or may request written copies, which will be provided for a nominal fee. (**Fees are listed under section j.**) The fee can be waived at the discretion of the right-to-know officer.
- 4) Shippensburg University will not create a public record that does not already exist, nor will it compile, maintain, format, or organize a public record in a manner in which the agency does not currently do so.

G. Responses

- 1) Types of responses.
 - a. The request is granted in its entirety.
 - b. The request is refused in its entirety.
 - c. The request is partially granted.

- 2) Deemed denials. The failure to make a timely response is deemed a denial.
- 3) Final responses granting requests.
 - a. A written request for a record will be granted if the record requested is within the statutory definition of a public record.
- 4) Final responses that deny requests, either in whole or in part.
 - a. A response that denies a request must list the entire specific reasons relied on for denying the request.
 - b. If a request is denied all or in part, the response must also contain a notice informing the requester of his or her right to file exceptions with the agency.
 - c. Any final response that sets forth a denial, whether in whole or in part, must contain the following:
 1. The name, title, business address, business telephone number and signature of the public official or employee on whose authority the denial is issued.
 2. The words "Mailing Date" followed by the date that is the mailing date of the response.
 3. A statement of the procedure that the requester may follow in order to file exceptions contesting the denial.
 - d. Grounds for a denial. A written request for access to, or a copy of, a record may be denied if any of the following circumstances exists:
 1. The requester is not a Pennsylvania resident.
 2. The requester has not identified any of the requested records with sufficient specificity.
 3. The record does not exist.
 4. The requester has not prepaid the costs of fulfilling the request, if the anticipated costs would exceed \$100.
 5. The record in question does not satisfy either prong of the Act's general definition of "public record."
 6. The record in question falls within one or more of the Act's statutory exceptions to the definition of "public record."
 - a. Disclosure of the institution, progress or results of an agency investigation.
 - b. Disclosure is prohibited, restricted or forbidden by statute, order or decree of court, or other law.

- c. Disclosure would operate to the prejudice or impairment of a person's reputation.
- d. Disclosure would operate to the prejudice or impairment of the security of one or more persons through the release of sensitive information. .
- e. Disclosure would result in the loss of federal funding.

H. Redaction.

- 1) Redaction means the eradication of a portion of a document while retaining the remainder. Redaction must be performed in such a way as to prevent the requester from having access to the redacted information.
- 2) If it is determined that a public record contains information subject to access, as well as information not subject to access, the Right-to-Know Law requires that the response must grant access to the information subject to access, but deny access to the information not subject to access.
- 3) The Office of Chief Counsel before delivery of the response will review any response that includes information that must be redacted.

I. Exceptions.

- 1) Exceptions intake procedures
 - a) Date-stamp the exceptions letter and assign it a tracking number.
 - b) Retain the envelope and any documents that accompany the exceptions letter.
 - c) Send a copy of the exceptions letter and accompanying documents to the person who signed the denial letter, in order to notify that person of the exceptions.
 - d) Send a copy of these materials to the right-to-know exemptions official.
 - e) Send a copy of these materials to legal counsel.
 - f) Maintain a record of the agency's final determination.
 - g) Prepare an official record in the event of an appeal to the Commonwealth Court.
- 2) Right to file exceptions.
 - a) Exceptions to a denial must be filed within 15 business days of the mailing date of the written denial.
 - b) Exceptions to a deemed denial must be filed within 15 calendar days of the date the request is deemed denied.
 - c) Exceptions that are untimely filed may be dismissed for that reasons.
- 3) Contents of exceptions.

- a) Exceptions must state the reasons upon which the requester asserts that the record is a public record. Reasons not set forth in writing within the applicable 15-day period are deemed to be waived and may be disregarded by the agency.
 - b) Exceptions should address the reasons stated by the agency for denying the request. Exceptions that fail to comply with this requirement may be dismissed for that reason.
- 4) Submission of exceptions.
- a) Exceptions must be set forth in writing and must be correctly addressed and submitted to the right-to-know exceptions officer. Exceptions submitted to any other official, office, or address are defective and do not stop the running of the 15-day exceptions period.

The exceptions officer for Shippensburg University is:

Dr. William N. Ruud, President
 Old Main 309
 Shippensburg University
 1871 Old Main Drive
 Shippensburg, PA 17257-2299
 FAX: (717) 477-4005

- b) Exceptions may be submitted by posting them through the U.S. mail. When this method is used, the mailing date is the date of the postmark on the envelope.
- c) If exceptions are filed in person, by facsimile transmission, by courier service, by overnight parcel delivery service, or in any way other than sending them through the U.S. mail, their mailing date is deemed to be the date the exceptions are received by the right-to-know exemptions officer.
- d) Exemptions may not be submitted by electronic mail.

J. Fees and charges

- 1) Photocopies. One "photocopy" is either a single-sided copy or one side of a double-sided copy.

I side of a standard 8.5 inch x 11 inch page	\$0.15 each
I side of any irregular sized page	\$0.20 each

- 2) PC diskettes \$1.00 each

- 3) Postage

Material fitting into standard letter envelope	No charge
Other	Actual cost

- 4) Electronic files delivered via electronic mail No charge

Checks for these costs should be made payable to Shippensburg University of Pennsylvania and include on the notation line "Right to Know Request."

Checks should be sent to:

Office of University Communications and Marketing

Old Main 306

Shippensburg University

1871 Old Main Drive

Shippensburg, PA 17257

rev. 6/1/2007

**Pennsylvania State System of Higher Education
Confidentiality Statement**

Background

With the implementation of the Shared Administrative System Human Resource/Payroll module using SAP technology, more information will be stored in electronic format. It is essential that the confidentiality and privacy of this information be maintained. As a Pennsylvania State System of Higher Education (System) employee who has been given access to confidential information, it is your responsibility to protect this sensitive and personal data.

System management and employees are relying on you to maintain confidentiality of the employee data and to access, use, discuss, release, and disclose this data only when it is dictated by your job duties. If you do not need to access employee information to perform your job, under no circumstances should it be accessed. If you do need to access employee information to perform your job, the information should not be divulged to anyone unless it is done so through authorized protocols.

To ensure that all System employees with access to SAP Human Resource/Payroll System information are aware of this confidentiality requirement, you must sign and date the statement below. You should retain a copy of this notice for your records and return the original copy of this form to your human resource office. If you have any questions regarding your responsibility to maintain confidentiality of the data to which you have access in your work associated with the SAP Human Resource/Payroll system, you should contact your human resource director.

Confidentiality Statement

As an employee of the Pennsylvania State System of Higher Education (System), I understand that I may have access to confidential, personal data of System employees. I agree that I will access, use, discuss, release, and/or divulge only the data that is needed to perform my job. I understand that I am prohibited from accessing, using, discussing, releasing, and/or divulging this data unless doing so is a requirement of my job. I understand that any release of this information will be done only through authorized protocols. For System employees, breaches in confidentiality of such data may result in disciplinary action up to and including separation from employment. A violation of this agreement also may result in legal action if it is determined that any local, state, or federal law has been violated.

By my signature below, I am certifying that I have read, understand, and agree to abide by the provisions of this policy.

Signature

Date

Printed Name

University

Confidentiality Statement

As an employee/student employee/graduate assistant of Shippensburg University of Pennsylvania I understand that I may have access to confidential, personal data and/or records of University employees, students, customers and other related constituents. I agree that I will access, use, discuss, release and/or divulge only the data that is needed to perform my job. I understand that I am prohibited from accessing, using, discussing, releasing, and/or divulging this data unless doing so is a requirement of my job.

I further understand that unauthorized disclosure of confidential information and records applies to all information on the University computing/networking systems, all printed information, as well as formal and informal verbal conversations.

I understand that any release of this information will be done only through authorized protocols. Breaches in confidentiality of such data may result in disciplinary action up to and including separation from employment and in the case of student employees and graduate assistants, possible University judicial action. A violation of this agreement also may result in legal action if it is determined that any local, state, or federal laws have been violated.

I have had the opportunity to discuss this responsibility with a representative of the University, and by my signature below, I am certifying that I have read, understand, and agree to abide by the provisions of this statement.

Name _____
(print)

Signature _____ Date _____

I have discussed the confidentiality statement with the above individual and he/she has acknowledged their understanding and acceptance of the above.

Name _____ Title _____
(print)

Signature _____ Date _____