University of Pittsburgh
Customer Information Security Plan

Purpose.

This information security plan describes the University of Pittsburgh's ongoing efforts to secure information related to students and others who provide certain sensitive information to the University. The University is required by law, specifically the federal Gramm-Leach-Bliley Act and its accompanying Safeguarding rule, the Federal Trade Commissions' s "Red Flags" rule, the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act ("HIPAA"), and the Pennsylvania Breach of Personal Information Notification Act to:

1) maintain, monitor, and test this plan;

2) designate a security officer to coordinate the safeguarding of customer information;

3) identify and assess risks to customer information;

4) evaluate, improve, and implement safeguards to protect customer information;

5) identify and respond to red flags concerning potential identity theft; and

6) notify individuals of data breaches under circumstances established by law.

The security plan also makes good business sense. This plan helps assure the University's "customers" that the university is taking adequate steps to protect their information and to minimize loss in the event of a security breach. The plan also serves to deter and respond to an increasingly common crime nationwide- identity theft.

Scope.

The security plan protects customer information University-wide in any office, department, school, or responsibility center that is significantly engaged in financial activities. When in doubt as to whether a school, department, responsibility center, or office is 'significantly engaged' in financial activities, the unit should err on the side of applicability.

"Customer information" means any paper or electronic record containing non-public personal information about an individual that the University, or its affiliates, handle and maintain. Customer information includes any personally identifiable information provided by students or others in order to obtain a financial product or service from the University such as loan applications, credit card numbers, account histories, and related consumer information. It also includes data found in accounts where the University provides services and defers payment (essentially extending credit) such as in a deferred tuition payment plan or ticket payment plan.

University Unit Responsibilities.

A. Securing Information.

Units must immediately and continually assess the safeguards they have in place to protect not only customer information- but all confidential University data. Heads of units should appoint a trusted and knowledgeable employee to oversee their individual safeguarding programs. Specific safeguarding practices that units must assess, and if necessary, implement, include:

1. Maintaining physical security by locking rooms and file cabinets where customer and sensitive information is stored. Ensuring windows are locked and using safes when practicable for especially sensitive data such as credit card information, checks, and currency;

2. Maintaining adequate key control and limiting access to sensitive areas to those individuals with appropriate clearance who require access to those areas as a result of their job;

3. Using and frequently changing passwords to access automated systems that process sensitive information and requiring identification before processing in-person transactions;

4. Using firewalls and encrypting information when feasible and using authentication and passwords when creating new accounts;

5. Referring calls and mail requesting customer information to those individuals who have been trained in safeguarding information;

6. Shredding and erasing customer information when no longer needed in accordance with unit and University policy and the law;

7. Encouraging employees to report suspicious activity to supervisors and law enforcement authorities;

8. Ensuring that agreements with third-party contractors contain safeguarding provisions and monitoring those agreements to oversee compliance;

9. Discouraging the use of social security numbers and using social security numbers only in accordance with university Policy on social security numbers;

10. Installing computer location software such as LoJack and using encryption and cable locks (if feasible) to secure all lap top computers.

B. Training.

1. Units should ensure that all new and existing employees who are involved in activities covered under this plan receive safeguarding and red flags training. A written agreement containing the employee's signature, and attesting to the fact that he or she received training, is aware of University and Unit information policies and guidelines, and is aware of the importance the University places on safeguarding information, is suggested. New users to Peoplesoft must receive the Introduction to Peoplesoft training, and user training increases for additional data access authority.

2. Training should, at a minimum, encompass the areas covered by this document.

C. Monitoring and Detection.

Units must continually assess what types of information are received, stored and distributed and assess the vulnerabilities of their systems. University consultants are available to assist in assessing the efficacy of their existing safeguards and in proposing improvements. The University Police, who have qualified security specialists on staff, are available to discuss physical security issues. CSSD will also provide a security analysis for your unit. Units should also identify particular red flags that may indicate that identify theft is afoot. These include:

1. Receipt of alerts from consumer reporting agencies such as a credit freeze or notice that certain accounts may be susceptible to fraud;
2. Receipt of suspicious documents containing forged signatures or apparent alterations or an identification card with a photograph that does not resemble the owner of the account;
3. Receipt of suspicious personal identifying information such as a Peoplesoft number that does not match the student, or information that matches somebody else's education records, or submitting a lack of required personal information after further request;
4. Unusual use of or other suspicious activity related to an account, such as recurring payment made to a student despite the student's not registering for courses, or refunds at unusual times, a pattern of dropping courses;
5. Receipt of notices from victims, law enforcement agencies, or others such as University administrators that an individual's information has been breached.

D. Managing Systems Failures and Handling Red Flags.

1. The University acknowledges that no system is flawless. Nevertheless, immediate steps should be taken to correct any security breach. Units must immediately report significant failures of their safeguarding system to the University Police, CSSD if the problem involves computer security, and to the Designated Customer information Security Officer. Affected customers may also need to be notified by University officials after the unit consults with the Designated Customer Information Security Office, University Police, and the Office of General Counsel about the necessity of notification and the proper notification procedures. Examples of significant failures would include a successful hacking effort that results in the loss of unencrypted personal data as defined Pennsylvania law, a burglary, or impersonations leading to the defrauding of customers.

2. Steps that units may take to respond to red flags it has detected or prevent a potential loss of data include: conducting an investigation, removing data from a network, monitoring accounts for evidence of identity theft, closing or re-designating accounts, refusing to open new accounts, contacting the customer after consultation with the above University officials, changing passwords, and further enhancing physical or computer security after consultation with University Police or CSSD.

E. No Third-Party Rights.

While this plan is intended to promote the security of information, it does not create any consumer, customer, or other third-party rights or remedies, or establish or increase any standards of care that would otherwise not be applicable.

University Policies and guidelines that Protect Customer Information.

The following policies and guidelines supplement and help to create a comprehensive information security plan. Referral and adherence to these documents is imperative to overall protection of customer information. The following documents are incorporated by reference into the plan.

A. University Policy and Procedure 09-08-01 govern "Access to Student Records." The policy and procedure outline the University's implementation of the Family Educational Rights and Privacy Act (FERPA). They can be found at:
http://www.bc.pitt.edu/policies/policy/09/09-08-01.html and
http://www.bc.pitt.edu/policies/procedure/09/09-08-01.html

B. The University's Registrar maintains an easy to read interpretation of FERPA as it applies to students' accounts at:
http://www.registrar.pitt.edu/ferpa.html
FERPA Training is also conducted upon departmental request and each term through the Office of Human Resources Faculty and Staff Development program.

C. University policy delineates the requirements and implementation of the Health insurance Portability and Accountability Act (HIPAA). This policy bolsters patient privacy in regard to health care and payment for health care, and can be found at:
http://www.pitt.edu/hipaa/ HIPAA training is conducted through an on-line module.

D. The University stresses information technology security in the following policies and guidelines:

University Policy and Procedure 10-02-04 governs access to data:
http://www.bc.pitt.edu/policies/policy/10/10-02-04.html and this is supplemented by role-based authorizations and training for the Peoplesoft student administration program;

University Policy 10-02-06 governs the security and privacy of University data and provides for disciplinary action against violators of the policy:
http://www.bc.pitt.edu/policies/policy/10/10-02-06.html

University Policy 10-02-08 governs the use and management of social security numbers and University Primary ID (UPI) Numbers:
http://www.bc.pitt.edu/policies/policy/10/10-02-08.html

The following guidelines also indicate how the University protects computer-based information.

General Computer Security and Tutorials:
http://technology.pitt.edu/security.html

E-Business Security Guidelines:
http://www.bc.pitt.edu/ebusiness/arEBSecurityGuide.pdf
and http://www.bc.pitt.edu/ebusiness/securityreview.htm

The Security Controls memorandum issued by Provost James V. Maher and Executive Vice Chancellor Jerome Cochran require all network-based firewalls for all University units:
http://technology.pitt.edu/Documents/security/Security_Controls_Memorandum.pdf

E. The University's Staff Handbook, in the Staff Responsibility section, emphasizes the protection and confidentiality of University proprietary information. It also specifically prohibits the misuse of information for personal gain or the gain of others in the Misuse of Information section. The Handbook is located at:
http://www.hr.pitt.edu/staff-handbook/

F. The University's Faculty Handbook, in the Misuse of Information section, prohibits faculty from unauthorized access to information for the purposes of personal gain or the gain of others. The handbook also stresses information security and is located at:
http://www.pitt.edu/~provost/handbook.html.

Designated Customer Information Security Officer.

The Designated Customer Information Security Officer is appointed by the Provost, and is responsible for coordinating the safeguarding of customer information throughout the University. Per the requirements of the Red Flags Rule, the Designated Customer Information Security Officer shall report annually to the Provost on the University units' adherence to this plan, effectiveness of the plan, serious incidents involving the use of the plan, related issues with third-part service providers, and any suggested material changes to the plan.