Scope of Policy and Rationale:

I. Gramm-Leach-Bliley Act; Federal Trade Commission Safeguards Rule. The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act ("GLBA" or "Act"), is a federal law that, among other things, regulates the security and confidentiality of customer nonpublic personal information possessed by financial institutions. Pursuant to the GLBA, the Federal Trade Commission ("FTC") has issued Standards for Safeguarding Customer Information (the "Safeguards Rule") that includes requirements for administrative, technical and physical information safeguarding of customer information. A copy of the Safeguards Rule is attached hereto as Exhibit A.

II. Comprehensive Information Security Program. Under FTC interpretation Temple University is subject to the GLBA by virtue of the university’s role in processing or servicing student loans as well as to the extent that it otherwise may provide financial products or services in conducting its activities. Accordingly, the university has established this Comprehensive Information Security Program (the “CISP”) to ensure compliance with the GLBA and applicable FTC regulations. A copy of the CISP may be obtained from the privacy officer identified in Exhibit B, or may be viewed on the

---


Temple University Policies and Procedures website. Supplementary information related to this policy is maintained by the privacy officer and can be found at http://www.temple.edu/privacy/.

III. Other Privacy and Information Security Laws and Policies. It is the policy of Temple University to comply and to require its employees to comply with all applicable federal, state and local laws and regulations and university policies and procedures governing the confidentiality, privacy and security of information. In addition to GLBA and the Safeguards Rule, other laws and regulations that regulate privacy and information security include:

- Family Educational Rights and Privacy Act of 1974 (“FERPA”)
- Health Insurance Portability and Accountability Act of 1996 (“HIPAA”)
- Pennsylvania Breach of Personal Information Notification Act (“PA SB 712”)
- Identity Theft Red Flags Rule (“Red Flags Rule”)
- Payment Card Industry – Data Security Standards (“PCI DSS”)

---

3 The Temple University Policies and Procedures can be found at http://policies.temple.edu
4 FERPA, also referred to as the “Buckley Amendment,” was enacted in 1974 and amended in 1990. The text of FERPA appears at 20 U.S.C. §1232g. Among other things, FERPA governs the privacy of student academic records. Federal regulations implementing FERPA appear at 34 CFR. Part 99. For more information see Temple University's Guidelines Pertaining to Confidentiality of Student Records (policy number 03.20.11) on the Temple University Policies and Procedures website.

5 Pub. L. 104-191. The U.S. Department of Health and Human Services issued Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 (“Privacy Rule”) to establish a set of national standards for the protection of certain health information. Discrete units within Temple University (direct providers of medical services, such as Student Health Services) have adopted internal policies regarding the confidentiality of student medical records. Those policies generally conform to the Temple University Health System, Inc. (“TUHS”) HIPAA policies. The TUHS Personal Health Information Privacy Practices Notice may be found at http://www.templehealth.org/content/HIPAA.asp.

6 PA Senate Bill No. 712 was enacted in 2005 to establish notification requirements for entities that experience a data breach that results in the exposure of private information. The bill includes definitions of personal information and has stipulations for when and how notifications are to be made.

7 The Red Flags Rule was developed pursuant to the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft. Temple University has established an Identity Theft Prevention Program (policy number 05.20.01).

8 The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, to help facilitate the broad adoption of consistent data security measures on a global basis. Temple University has established a Credit Card Handling and Acceptance Policy (policy number 05.20.17).
Temple University has implemented guidelines and policies regarding FERPA, HIPAA as well as Social Security Number (“SSN”) usage policy and procedures. This CISP does not replace or supersede, but rather is intended to complement (and should be interpreted consistently with) other university policies that deal with privacy and information security.

IV. Safeguards Rule Requirements and CISP Objectives. The objectives of Section 501(b) of the GLBA and the Safeguards Rule standards are to:

1. Ensure the security and confidentiality of customer records (see Section V. Scope of CISP below);
2. Protect against any anticipated threats or hazards to the security or integrity of such records; and
3. Protect against unauthorized access to or use of such records that could result in substantial harm or inconvenience to any customer.

This CISP is designed to ensure compliance with the Safeguards Rule and other laws and regulations applicable to the protection of customer nonpublic personal information.

V. Scope of CISP.

This CISP applies to any record, handled or maintained by or on behalf of the university that contains nonpublic personal information about a “customer” in connection with a transaction involving a financial product or service provided by the university. Specifically, a “customer” is (i) a student who applies for or receives a student loan or (ii) a donor who enters into a gift annuity arrangement with the university.

Questions about whether other transactions involve a financial product or service, or whether personal information was obtained in connection with a financial product or service, should be referred to the privacy officer.

VI. Definitions.

a. “Consumer” means an individual (or an individual’s legal representative) who obtains or has obtained a financial product or service from the University that is to be used primarily for personal, family, or household purposes.

---

9 The Social Security Number Usage Policy (policy number 04.75.11) and the Social Security Number Usage Procedures (policy number 04.75.12) can be found on the Policies and Procedures website.
10 15 U.S.C. 6801(b)(1) - (3).
11 The record may be in paper, electronic or other form.
b. “Covered data field” means any part of a customer’s record that contains nonpublic personal information as defined by this CISP.

c. “Covered record” means any customer record that contains a covered data field.

d. “Covered Unit” means any university department that is subject to this CISP.

e. “Covered Individual” means any individual subject to this CISP whose conduct, in the performance of work for Temple University, is under the direct control of Temple University.

f. “Customer” generally means a consumer who has a customer relationship with the university.

g. “Customer relationship” means a continuing relationship between a consumer and the university under which the university provides one or more financial products or services to the consumer to be used primarily for personal, family, or household purposes.

h. “Customer Information” means any record containing nonpublic personal information.

i. “Data Handbook” means a listing of those persons or offices responsible for each covered data field.

j. “Nonpublic personal information” means:
   i. personally identifiable financial information and
   ii. any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available (“Nonpublic List”).

k. “Personally identifiable financial information” means any information:
   i. a consumer provides to the university to obtain a financial product or service from or through the university
   ii. about a consumer resulting from any transaction involving a financial product or service between the university and the consumer, or
   iii. the University otherwise obtains about a consumer in connection with providing a financial product or service to that consumer. Personally identifiable financial information does not include publicly available information, except as included on a nonpublic list.

l. “Registry” means a listing of those persons who have access to covered data fields.

Terms not defined in this CISP shall, unless the context clearly requires otherwise, take the meaning ascribed by applicable FTC regulations, primarily found in the Safeguards Rule and the Privacy of Consumer Financial Information\(^\text{12}\) (the “Privacy Rule”).\(^\text{13}\) A

\(^{12}\) 16 CFR Chapter I, Subchapter C, Part 313, Section 313.3.

\(^{13}\) Particularly important terms defined in the Privacy Rule are: "consumer", "customer", "customer information", "financial product or service", "nonpublic personal information", "personally identifiable financial information" and "publicly available information" and terms defined in the Safeguards Rule are "service provider"
copy of the Privacy Rule is attached hereto as Exhibit C. Terms defined in this CISP, shall to the extent possible, be read consistently with the definitions provided for those same terms in the applicable FTC regulations.

VII. Safeguards. All employees with access to customer nonpublic personal information and business associates with access to such information (“Covered Individuals”) shall treat that customer nonpublic personal information with due care and respect for its privacy and confidentiality. In doing so, the covered individual shall comply with this CISP and, in particular, the university administrative, technical and physical safeguards set forth in Exhibit D attached hereto and any additional administrative, technical and physical safeguards that are applicable to that covered individual’s unit.

VIII. Privacy Officer. The designated employee responsible for the overall coordination and implementation of this CISP is the privacy officer of Temple University. The privacy officer may, subject to the approval of the vice president for computer and financial services, and chief information officer, request that other representatives of the University accept responsibility to oversee and coordinate particular elements of this CISP. Any questions regarding the implementation of this CISP or the interpretation of this document should be directed to the Privacy Officer or his or her designees. Contact information for the privacy officer is set forth on Exhibit B.

The Privacy Officer shall:

1. Coordinate with the management audit committee, internal audits, university counsel, vice president for computer and financial services, and chief information officer, and the chief information security officer to maintain this CISP.
2. Provide guidance in complying with all privacy safeguarding regulations (in consultation with the Offices of University Counsel and/or vice president for computer and financial services, and chief information officer as appropriate).
3. Critically evaluate the design, operation and oversight of this CISP and submit to the Management Audit Committee not less than annually a university risk assessment (see section XII Risk Assessment below).
4. Coordinate with Human Resources and appropriate covered units to deliver employee training on the university's procedures and practices relating to access to and use of nonpublic personal information, particularly student and employee records including financial aid and loan information.
5. Coordinate with the chief information security officer regarding the security controls of information systems and log data surrounding an information systems’ attack or breach.

and "information security program".
6. Have the option, in consultation with the chief information security officer, to delegate to a representative of the Office of Computer and Information Services the responsibility for monitoring and participating in the dissemination of information related to the reporting of known attacks and other threats to the integrity of networks utilized by the university.

IX. Covered Units.

Each Covered Unit shall:

1. Designate employees who will act as information privacy and security liaisons. These individuals will work with the privacy officer, chief information security officer and Internal Audits, and will represent their department with respect to information privacy, security and compliance. These liaisons should be sufficiently qualified to coordinate all activities related to information privacy and security, and to ensure that the covered unit meets requirements of this CISP.

2. Be responsible for securing customer nonpublic personal information in accordance with this CISP and all applicable privacy laws, regulations, policies, programs, procedures, standards and guidelines.

3. Maintain a registry of covered individuals working in or for the covered unit.

4. Consistent with this CISP (with guidance from the privacy officer where required), determine what information entrusted to or accessible by the covered unit is private and/or confidential; and communicate, to appropriate persons associated with the unit, methods of protecting that information (from acquisition through destruction).

5. Implement such additional safeguards in accordance with the nature and scope of the unit's activities and the sensitivity of any customer nonpublic personal information at issue.

6. Maintain a written security program that details such additional safeguards and provide a copy of that program to the privacy officer.

7. Identify computers (laptops, workstations and servers) on which customer nonpublic personal information is stored or accessed, or from which such information is transmitted; ensure that these systems are evaluated (with the guidance of the chief information security officer where needed) at least annually for physical and technical vulnerabilities, using methods that are consistent with accepted industry standards.

8. Assure that patches for operating systems or software environments not under the direct control or management of Computer and Information Services are up to date, and keep records of patching activity.

9. Conduct, no less than annually, a risk assessment that critically evaluates risk of exposure of customer nonpublic personal information, and submits copies of this report to the units’ cognizant vice president or provost, and
the privacy officer. This report should include all administrative, technical and physical safeguards that have been implemented to significantly reduce or eliminate risk (refer to Section XII for more information).

10. In the event of a data breach that exposes customer information, the covered unit must immediately notify the privacy officer or the chief information security officer. The covered unit must cooperate fully, and must assign human and financial resources during the breach remediation and notification process.

X. Covered Individual Responsibilities and Training. The university will hold covered individuals accountable for maintaining confidentiality of customer nonpublic personal information. Covered Individuals generally can be classified as: information technologists who have access (with no or limited restrictions) to such information; custodians of data as identified in the Data Handbook (see Section XIV Computer Services), and those who use the information as part of their essential job duties. The privacy officer will work with the relevant covered units to develop and maintain a registry of covered individuals. The privacy officer, in cooperation with Human Resources and the relevant covered units, will work to continuously update the registry.

Managers and/or privacy and security liaisons of covered units shall ensure that covered individuals receive adequate training regarding this CISP and applicable safeguards at least annually. Covered individuals should receive uniform training on the handling of non public personal information that is consistent with guidance provided by the university privacy officer and the chief information security officer. New employees, an actual disclosure, or sensitive positions may necessitate more frequent training or review, and each covered unit should tailor its training to address its particular needs. Current potential threats to customer information should be covered, as well as how employees are expected to address these issues with university customers. Training also should include controls and procedures to prevent employees from providing customer information to an unauthorized individual (including "pretext calling – a.k.a. social engineering"), and how to properly dispose of documents that contain nonpublic personal information. As necessary, other training shall be provided to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures. The goal of this training is to minimize risk and safeguard customer information.

Breach of confidentiality or other noncompliance with the CISP may result in internal disciplinary or other corrective action as well as the possibility of civil or criminal prosecution or, with respect to third party vendors, contract remedies. Employees who know or suspect that confidentiality has been breached have a responsibility to report the breach to their supervisor, privacy officer or the chief information security officer. All faculty, staff, administrators, volunteers, trainees, students, independent contractors must
cooperate fully with those performing an authorized investigation pursuant to this CISP.

XI. **Risk Review.** Each covered unit shall conduct an annual risk review to assess new risks and shall update internal controls and safeguards accordingly. Based on the risk review, each covered unit shall submit an annual risk assessment (refer to section xii for more details) to the privacy officer. The privacy officer shall review the covered unit’s annual risk assessment and conduct an annual overall university risk assessment for presentation to the Management Audit Committee.

XII. **Risk Assessment.** A risk assessment seeks to identify foreseeable internal and external risks to the security, confidentiality, and integrity of customer nonpublic personal information that could result in unauthorized disclosure, misuse, alteration or destruction or other compromise of such information. The risk assessment should, at a minimum, include considerations of risks and management of those risks including: employee training and management; information systems (including network and software design, as well as information processing, storage, transmission and disposal); and detecting, preventing and responding to attacks, intrusions, or other system failures. Risk assessments should include a report of implemented safeguards and indicate how frequently tests are conducted to monitor the effectiveness of the safeguards’ key controls, systems, and procedures.

In implementing this CISP, the privacy officer, working with the chief information security officer, will establish procedures for identifying and assessing such risks in each covered unit. Specific areas of risks to be assessed include: unauthorized access and/or use of customer nonpublic personal information by means of computer and electronic data or paper documents and files, unauthorized access and/or use of personal customer information by third party vendors, and unauthorized access to the data processing or telephone communication system. Each covered unit shall perform an initial risk assessment. The privacy officer shall perform an overall risk assessment of the university.

XIII. **Assessment and Review Reporting.** Each covered unit shall submit a report of its initial risk assessment and, thereafter, an annual risk assessment to the privacy officer. The privacy officer shall conduct an initial risk assessment of the university and, thereafter, an annual risk assessment of the university. Internal Audits shall perform spot checks of the privacy officer’s and selected covered units’ risk assessments on a periodic basis, and report its findings to the Management Audit Committee. The Office of Computer Services shall assist the privacy officer and Internal Audits with respect to information systems, attacks, technology safeguards and information technology issues in risk assessments. Reports or portions of reports of risk assessments shall remain confidential if dissemination of those reports or portions reasonably might lead to breaches of security or privacy.
XIV. **Computer Services.** The Office of Computer Services should:

1. Develop and maintain policies and procedures that protect against any anticipated threats to the security or integrity of customer nonpublic personal information in electronic form and that guard against the unauthorized use of such information.
2. Provide guidance to covered units in developing individual units’ information security safeguards.
3. Upon request by covered units, monitor computer systems that store non public personal information and report any successful attempts that have been made by unauthorized individuals to gain access to these systems; monitor networks and review system computer maintenance reports to ascertain whether any unauthorized changes have occurred to customer account information or personal data; and develop written plans and incident response procedures for dealing with such attempts and occurrences.
4. File a suspicious activity report if inappropriate access to or unauthorized disclosure of information is suspected or unauthorized activity is attempted by an unauthorized individual.
5. In cooperation with relevant covered units develop and maintain a data handbook, listing those persons or offices responsible for each covered data field in relevant information systems.
6. Assure that patches for operating systems or software environments under its direct management/control are reasonably up to date, and keep records of patching activity. Implement technical controls to mitigate or prevent vulnerabilities and attacks.
7. Explore the feasibility of plans to promote the encryption of electronic nonpublic personal information in transit.
8. Protect central databases from security risks.
9. Periodically review the university's disaster recovery program and applicable data retention policies and present a report to the privacy officer.

XV. **Service Providers.** A service provider is any person or entity that receives, maintains, processes, or otherwise is permitted access to nonpublic customer information through its provision of services directly to Temple University. The applicable covered units shall take reasonable steps to: select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue; and contract with all service providers to implement and maintain the identified safeguards in accordance with Exhibit E (attached hereto and incorporated herein). The privacy officer shall coordinate with University Counsel and such covered units and other affected units to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for customer nonpublic financial information to which they will have access.

See generally 16 CFR 314.2(d).
XVI. **No Third Party Rights.** While this CISP is intended to promote the protection of customer information, this CISP does not (i) create any consumer, customer or other third party rights or remedies or (ii) establish or increase any standards of care that would not otherwise be applicable upon which any such third party may rely.

XVII. **CISP Modifications.** The privacy officer shall evaluate this CISP (i) in light of relevant circumstances (including changes in applicable laws and regulations and the university's business arrangements or operations), (ii) based upon periodic testing and monitoring of this CISP’s effectiveness in terms of its key controls, systems, and procedures and (iii) in comparison with available programs widely practiced at other selected national research universities. In consultation with the Office of Computer Services, university counsel and Internal Audits, the privacy officer shall then recommend to the Management Audit Committee any appropriate adjustments to this CISP.

XVIII. **Questions and Additional Information.**

For clarification or more information, contact the privacy officer (contact information appears on Exhibit B) after carefully reviewing this CISP, including the safeguards contained in Exhibit D and service provider provisions in Exhibit E, as appropriate.

1. **Dates of official enactment and amendments:**

   August 12, 2003

2. **History:**

   Revised: March 25, 2009

3. **Cross References**

   Social Security Number Usage policy 04.75.11
   [http://policies.temple.edu/getdoc.asp?policy_no=04.75.11](http://policies.temple.edu/getdoc.asp?policy_no=04.75.11)
   Social Security Number Usage Procedures 04.75.12
   [http://policies.temple.edu/getdoc.asp?policy_no=04.75.12](http://policies.temple.edu/getdoc.asp?policy_no=04.75.12)
   Identity Theft Prevention Program 05.20.01
   [http://policies.temple.edu/getdoc.asp?policy_no=05.20.01](http://policies.temple.edu/getdoc.asp?policy_no=05.20.01)
   Credit Card Handling and Acceptance policy 05.20.17
   [http://policies.temple.edu/getdoc.asp?policy_no=05.20.17](http://policies.temple.edu/getdoc.asp?policy_no=05.20.17)
List of Subjects for 16 CFR Part 314

Consumer protection, Credit, Data protection, Privacy, Trade practices.

Final Rule

For the reasons set forth in the preamble, the Federal Trade Commission amends 16 CFR chapter I, subchapter C, by adding a new part 314 to read as follows:

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Sec.
314.1 Purpose and scope.
314.2 Definitions.
314.3 Standards for safeguarding customer information.
314.4 Elements.
314.5 Effective date.


§314.1 Purpose and scope.
(a) Purpose. This part, which implements sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act, sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

(b) Scope. This part applies to the handling of customer information by all financial institutions over which the Federal Trade Commission ("FTC" or "Commission") has jurisdiction. This part refers to such entities as "you." This part applies to all customer information in your possession, regardless of whether such information pertains to individuals with whom you have a customer relationship, or pertains to the customers of other financial institutions that have provided such information to you.

§314.2 Definitions.
(a) In general. Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Commission's rule governing the Privacy of Consumer Financial Information, 16 CFR part 313.

(b) Customer information means any record containing nonpublic personal information as defined in 16 CFR 313.3(n), about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.
(c) Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

(d) Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

§314.3 Standards for safeguarding customer information.

(a) Information security program. You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:

(1) Insure the security and confidentiality of customer information;
(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

§314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security program.

(b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;
(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

§314.5 Effective date.

(a) Each financial institution subject to the Commission's jurisdiction must implement an information security program pursuant to this part no later than May 23, 2003.

(b) Two-year grandfathering of service contracts. Until May 24, 2004, a contract you have entered into with a nonaffiliated third party to perform services for you or functions on your behalf satisfies the provisions of §314.4(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as you entered into the contract not later than June 24, 2002.

By direction of the Commission.

Donald S. Clark,
Secretary.

[FR Doc. 02–12952 Filed 5–22–02; 8:45 am]

BILLING CODE 6750–01–P
EXHIBIT B

UNIVERSITY PRIVACY OFFICER

Name: Robert M. Edamala

Mailing Address: University Privacy Officer
Temple University
The TECH Center, Room 408
1101 West Montgomery Avenue
Philadelphia, PA 19122

Telephone Number: (215) 204-6596

Fax Number: (215) 204-0535

Email Address: robert.edamala@temple.edu

Web Address: http://www.temple.edu/privacy
§313.3 Definitions.

As used in this part, unless the context requires otherwise:

(a) Affiliate means any company that controls, is controlled by, or is under common control with another company.

(b)(1) Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice.

(2) Examples—(i) Reasonably understandable. You make your notice reasonably understandable if you:

(A) Present the information in the notice in clear, concise sentences, paragraphs, and sections;

(B) Use short explanatory sentences or bullet lists whenever possible;

(C) Use definite, concrete, everyday words and active voice whenever possible;

(D) Avoid multiple negatives;

(E) Avoid legal and highly technical business terminology whenever possible; and

(F) Avoid explanations that are imprecise and readily subject to different interpretations.

(ii) Designed to call attention. You design your notice to call attention to the nature and significance of the information in it if you:

(A) Use a plain-language heading to call attention to the notice;

(B) Use a typeface and type size that are easy to read;

(C) Provide wide margins and ample line spacing;

(D) Use boldface or italics for key words; and

(E) In a form that combines your notice with other information, use distinctive type size, style, and graphic devices, such as shading or sidebars, when you combine your notice with other information.

(iii) Notices on websites. If you provide a notice on a web page, you design your notice to call attention to the nature and significance of the information in it if you use text or visual cues to encourage scrolling down the page if necessary to view the entire notice and ensure that other elements on the web site (such as text, graphics, hyperlinks, or sound) do not distract attention from the notice, and you either:

(A) Place the notice on a screen that consumers frequently access, such as a page on which transactions are conducted; or

(B) Place a link on a screen that consumers frequently access, such as a page on which transactions are conducted, that connects directly to the notice and is labeled appropriately to convey the importance, nature and relevance of the notice.

(c) Collect means to obtain information that you organize or can retrieve by the name of an individual or by identifying number, symbol, or other identifying particular assigned to the individual, irrespective of the source of the underlying information.

(d) Company means any corporation, limited liability company, business trust, general or limited partnership, association, or similar organization.

(e)(1) Consumer means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes, or that individual’s legal representative.

(2) Examples—(i) An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.

(ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.

(iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or
economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

(iv) If you hold ownership or servicing rights to an individual’s loan that is used primarily for personal, family, or household purposes, the individual is your consumer, even if you hold those rights in conjunction with one or more other institutions. (The individual is also a consumer with respect to the other financial institutions involved.) An individual who has a loan in which you have ownership or servicing rights is your consumer, even if you, or another institution with those rights, hire an agent to collect on the loan.

(v) An individual who is a consumer of another financial institution is not your consumer solely because you act as agent for, or provide processing or other services to, that financial institution.

(vi) An individual is not your consumer solely because he or she has designated you as trustee for a trust.

(vii) An individual is not your consumer solely because he or she is a beneficiary of a trust for which you are a trustee.

(viii) An individual is not your consumer solely because he or she is a participant in an employee benefit plan that you sponsor or for which you act as a trustee or fiduciary.

(f) Consumer reporting agency has the same meaning as in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f)).

(g) Control of a company means:

(1) Ownership, control, or power to vote 25 percent or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

(2) Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or

(3) The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company.

(h) Customer means a consumer who has a customer relationship with you.

(i) Customer relationship means a continuing relationship between a consumer and you under which you provide one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes.

(2) Examples—(i) Continuing relationship. A consumer has a continuing relationship with you if the consumer:

(A) Has a credit or investment account with you;

(B) Obtains a loan from you;

(C) Purchases an insurance product from you;

(D) Holds an investment product through you, such as when you act as a custodian for securities or for assets in an individual retirement arrangement;

(E) Enters into an agreement or understanding with you whereby you undertake to arrange or broker a home mortgage loan, or credit to purchase a vehicle, for the consumer;

(F) Enters into a lease of personal property on a non-operating basis with you;

(G) Obtains financial, investment, or economic advisory services from you for a fee;

(H) Becomes your client for the purpose of obtaining tax preparation or credit counseling services from you;

(I) Obtains career counseling while seeking employment with a financial institution or the finance, accounting, or audit department of any company (or while employed by such a financial institution or department of any company);

(J) Is obligated on an account that you purchase from another financial institution, regardless of whether the account is in default when purchased, unless you do not locate the consumer or attempt to collect any amount from the consumer on the account;

(K) Obtains real estate settlement services from you; or

(L) Has a loan for which you own the servicing rights.

(ii) No continuing relationship. A consumer does not, however, have a continuing relationship with you if:

(A) The consumer obtains a financial product or service from you only in isolated transactions, such as using your ATM to withdraw cash from an account at another financial institution; purchasing a money order from you; or making a wire transfer through you;

(B) You sold the consumer’s loan and do not retain the rights to service that loan;

(C) You sold the consumer airline tickets, travel insurance, or traveler’s checks in isolated transactions;

(D) The consumer obtains one-time personal or real property appraisal services from you; or

(E) The consumer purchases checks for a personal checking account from you.

(ii) Federal functional regulator means:

(1) The Board of Governors of the Federal Reserve System;

(2) The Office of the Comptroller of the Currency;

(3) The Board of Directors of the Federal Deposit Insurance Corporation;

(4) The Director of the Office of Thrift Supervision;

(5) The National Credit Union Administration Board; and


(k)(1) Financial institution means any institution the business of which is engaged in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)). An institution that is significantly engaged in financial activities is a financial institution.

(2) Examples of financial institution.

(i) A retailer that extends credit by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(f) of the Bank Holding Company Act and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) A personal property or real estate appraiser is a financial institution because real and personal property appraisals are a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(f) of the Bank Holding Company Act.

(iii) An automobile dealership that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(f) of the Bank Holding Company Act.

(iv) A career counselor that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting, or audit departments of any company is a financial institution because such career counseling activities are financial activities listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(f) of the Bank Holding Company Act.

(v) A business that prints and sells checks for consumers, either as its sole business or as one of its product lines,
is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(vi) A business that regularly wires money to and from consumers is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A check cashing business is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act.

(viii) An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(ix) A business that operates a travel agency in connection with financial services is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 211.5(d)(15) and referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(x) An entity that provides real estate settlement services is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xi) A mortgage broker is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act.

(xii) An investment advisory company and a credit counseling service are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act.

(3) Financial institution does not include:

(i) Any person or entity with respect to any financial activity that is subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (7 U.S.C. 1 et seq.);

(ii) The Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.); or

(iii) Institutions chartered by Congress specifically to engage in securitizations, secondary market sales (including sales of servicing rights) or similar transactions related to a transaction of a consumer, as long as such institutions do not sell or transfer nonpublic personal information to a nonaffiliated third party other than as permitted by §§ 313.14 and 313.15 of this part.

(iv) Entities that engage in financial activities but that are not significantly engaged in those financial activities.

(4) Examples of entities that are not significantly engaged in financial activities. (i) A retailer is not a financial institution if its only means of extending credit are occasional “lay away” and deferred payment plans or accepting payment by means of credit cards issued by others.

(ii) A retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue.

(iii) A merchant is not a financial institution merely because it allows an individual to “run a tab.”

(iv) A grocery store is not a financial institution merely because it allows individuals to whom it sells groceries to cash a check, or write a check for a higher amount than the grocery purchase and obtain cash in return.

(m)(1) Nonaffiliated third party means any person except:

(i) Your affiliate; or

(ii) A person employed jointly by you and any company that is not your affiliate (but nonaffiliated third party includes the other company that jointly employs the person).

(2) Nonaffiliated third party includes any company that is an affiliate by virtue of your or your affiliate’s direct or indirect ownership or control of the company in conducting merchant banking or investment banking activities of the type described in section 4(k)(4)(H) or insurance company investment activities of the type described in section 4(k)(4)(I) of the Bank Holding Company Act (12 U.S.C. 1843(k)(4)(H) and (I)).

(u)(1) Nonpublic personal information means:

(i) Personally identifiable financial information; and

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

(2) Nonpublic personal information does not include:

(i) Publicly available information, except as included on a list described in paragraph (u)(1)(i) of this section; or

(ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

(3) Examples of lists—(i) Nonpublic personal information includes any list of individuals’ names and street addresses that is derived in whole or in part using personally identifiable financial information (that is not publicly available), such as account numbers.

(ii) Nonpublic personal information does not include any list of individuals’ names and addresses that contains only publicly available information, is not derived, in whole or in part, using personally identifiable financial information that is not publicly available, and is not disclosed in a manner that indicates that any of the individuals on the list is a consumer of a financial institution.

(o)(1) Personally identifiable financial information means any information:

(i) A consumer provides to you to obtain a financial product or service from you;

(ii) About a consumer resulting from any transaction involving a financial product or service between you and a consumer; or

(iii) You otherwise obtain about a consumer in connection with providing a financial product or service to that consumer.

(2) Examples—(i) Information included. Personally identifiable financial information includes:

(A) Information a consumer provides to you on an application to obtain a loan, credit card, or other financial product or service;

(B) Account balance information, payment history, overdraft history, and credit or debit card purchase information;

(C) The fact that an individual is or has been one of your customers or has

Exhibit C - Privacy Rule (definitions)
obtained a financial product or service from you;
(D) Any information about your consumer if it is disclosed in a manner that indicates that the individual is or has been your consumer;
(E) Any information that a consumer provides to you or that you or your agent otherwise obtain in connection with collecting on, or servicing, a credit account;
(F) Any information you collect through an Internet “cookie” (an information collecting device from a web server); and
(G) Information from a consumer report.
(ii) Information not included. Personally identifiable financial information does not include:
(A) A list of names and addresses of customers of an entity that is not a financial institution; and
(B) Information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses.
(p)(1) Publicly available information means any information that you have a reasonable basis to believe is lawfully made available to the general public from:
(i) Federal, State, or local government records;
(ii) Widely distributed media; or
(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.
(2) Reasonable basis. You have a reasonable basis to believe that information is lawfully made available to the general public if you have taken steps to determine:
(i) That the information is of the type that is available to the general public; and
(ii) Whether an individual can direct that the information not be made available to the general public and, if so, that your consumer has not done so.
(3) Examples—(i) Government records. Publicly available information in government records includes information in government real estate records and security interest filings.
(ii) Widely distributed media. Publicly available information from widely distributed media includes information from a telephone book, a television or radio program, a newspaper, or a website that is available to the general public on an unrestricted basis. A website is not restricted merely because an Internet service provider or a site operator requires a fee or a password, so long as access is available to the general public.
(iii) Reasonable basis—(A) You have a reasonable basis to believe that mortgage information is lawfully made available to the general public if you have determined that the information is of the type included on the public record in the jurisdiction where the mortgage would be recorded.
(B) You have a reasonable basis to believe that an individual’s telephone number is lawfully made available to the general public if you have located the telephone number in the telephone book or the consumer has informed you that the telephone number is not unlisted.
(q) You include each “financial institution” (but excludes any “other person”) over which the Commission has enforcement jurisdiction pursuant to section 505(a)(7) of the Gramm-Leach-Bliley Act.

Exhibit C - Privacy Rule (definitions)
EXHIBIT D

SAFEGUARDS

All employees with access to customer nonpublic personal information shall comply with University administrative, technical and physical safeguards set forth below and any additional administrative, technical and physical safeguards that are applicable to that employee's unit.

Administrative Safeguards

1. Covered Units shall classify and label, as appropriate, documents or customer information as to confidentiality and sensitivity.
2. Covered Units shall follow reasonable guidelines or otherwise employ due care for the release and other handling of customer information.
3. Human Resources should generally conduct background checks on prospective employees to whom access would be granted (i.e., those who would become a Covered Individual). Covered Units should notify Human Resources of the need for the background check.
4. Authorization for access to specific nonpublic personal information shall be granted only to Covered Individuals and only on a “need-to-know” basis.
5. Covered Units shall provide timely information to the Privacy Officer and Human Resources regarding additions to, deletions from and other changes to the Registry.
6. Covered Units shall follow applicable disaster recovery/business continuity and emergency procedures.

Physical Safeguards

1. Covered Units shall follow reasonable guidelines for the creating, amending, accessing, storing, processing, transmitting, and disposing of hard copy records (e.g., paper documents that contain nonpublic personal information shall be shredded before disposal).
2. Covered Units shall follow procedures for protecting hard copy documents, files, electronic storage media, and hardware (computers, disk and non-disk media, terminals, printers, peripherals, etc.) from damage, theft and unauthorized access.
3. All student loan promissory notes shall be maintained in fireproof file cabinets as mandated under federal regulations.
4. All other student financial aid and student loan borrower records shall be maintained in a secure walk-in filing system.
5. Covered Units with financial aid and student loan borrower records should:
   A. Lock the office doors with the last person leaving the office setting an alarm (alarm codes should be individualized to authenticate each office staff member).
   B. Lock the filing system each evening before the office is closed.
   C. File in the walk-in filing system any records copied or printed out for use on a daily basis, in a secure area.
   D. In a secure manner destroy any duplicate and unnecessary records.
6. Covered Units shall follow applicable disaster recovery/business continuity and emergency procedures.

Technical Safeguards

1. Computer Usage Policy.
   (http://policies.temple.edu/getdoc.asp?policy_no=04.71.11)
2. Computer Services Department’s Computer and Network Security Policy.
   (http://policies.temple.edu/getdoc.asp?policy_no=04.72.12)
3. Applicable disaster recovery/business continuity and emergency procedures.

All other applicable policies, procedures, guidelines, standards and the like for creating, amending, accessing, storing, processing, transmitting, and disposing of electronic records can be found on the following websites:

1. Temple University Policy Website
   (http://policies.temple.edu)
2. Information Security Website
   (http://www.temple.edu/cs/security)
3. University Privacy Officers Website
   (http://www.temple.edu/privacy)
4. Federal Trade Commission Website
   (http://www.ftc.gov/privacy/privacyinitiatives/safeguards_educ.html)
EXHIBIT E

SERVICE PROVIDER REQUIREMENTS

Pursuant to the Agreement, _____________________________ (“Service Provider”) is a service provider to whom Temple University (“Temple” or the “University”) shall provide access to nonpublic personal information. Service Provider shall provide adequate safeguards for the protection of the confidentiality of such information. As applicable, those safeguards shall conform to the requirements of the Gramm-Leach-Bliley Act\(^\text{15}\) (“GLBA”) and the Federal Trade Commission’s *Standards for Safeguarding Customer Information*\(^\text{16}\) (the “Safeguards Rule,” a copy of which is attached hereto). The confidentiality, security and other requirements set forth in this Exhibit (the “Service Provider Requirements”) shall comprise the minimum safeguards to be employed by Service Provider.

1. **Definitions**

1.1 "Confidential information" means any information and documents, (including, without limitation, data, educational materials, materials relating to business, protocols, guidelines, pricing, strategies, compensation levels, financial information, nonpublic personal information, trade secrets, and technology), in any form (e.g., electronic, paper, or other) concerning Temple University, its affiliates or any Temple Community Members that are submitted under this Agreement or which Service Provider becomes aware of during the course of its performance hereunder are confidential and proprietary to Temple University.

1.2 "Nonpublic personal information" takes the meaning provided in the Federal Trade Commission’s *Privacy of Consumer Financial Information*\(^\text{17}\) (the “Privacy Rule,” a portion of which is attached hereto), except that in this context nonpublic personal information is not limited to information about customers or consumer of Temple University that seek or are provided financial products or services, but rather nonpublic personal information includes information about Temple Community Members regardless of whether they seek or obtain any financial product or service. Examples of nonpublic personal information include the following: Temple Community Member's social security number, address, grades, employment data and any other personally identifiable information that if disclosed without authorization might result in substantial harm or inconvenience.


\(^{16}\) 16 CFR Part 314, Standards for Safeguarding Customer Information.

\(^{17}\) 16 CFR Chapter I, Subchapter C, Part 313, Section 313.3.
1.3 "Temple Community Members" means current or former or prospective trustees, officers, faculty, staff, employees, students, volunteers, agents, or representatives of Temple University or its affiliates.

2. Confidentiality and Nondisclosure

Service Provider shall hold all Confidential Information in the strictest confidence and in accordance with applicable laws and regulations as well as Temple University's policies and procedures. Service Provider shall obtain no proprietary rights (directly or indirectly) in or to the Confidential Information. Service Provider shall not disclose the Confidential Information to any third party without the prior written consent of Temple University unless (i) required to perform Service Provider's obligations under the Agreement or (ii) required by law in which event Service Provider shall promptly notify Temple University of such request. Service Provider shall use such Confidential Information only in connection with the furtherance of the business relationship between the parties, and Service Provider shall make no further use, in whole or in part, of any such Confidential Information. Service Provider further agrees to disclose the Confidential Information only to its employees whose services are required in furtherance of the objectives of the business relationship between the parties, and to require each of its employees to comply with the terms of this Agreement, prior to the disclosure to such employees. Upon the expiration or termination of this Agreement, for any reason, Service Provider shall promptly turn over and return to Temple University all Confidential Information (in whatever form or media) or upon the written direction of Temple University, destroy the Confidential Information.

3. Service Provider Safeguards Report

Service Provider has submitted a report (the “Service Provider Safeguards Report,” a copy of which is attached hereto) to the University that defines what steps Service Provider is taking and shall take to protect University customer information. Service Provider shall review the Service Provider Safeguards Report and revise as appropriate not less than annually. Service Provider shall comply with the requirements included in the Service Provider Safeguards Report. The University’s Privacy Officer may annually (or more frequently as circumstances require in the Privacy Officer’s judgment) conduct a review of Service Provider's compliance with the Service Provider Safeguards Report, Service Provider Requirements, GLBA and Safeguards Rule.
4. **Service Provider Agreements, Acknowledgments, Representations and Warranties**

Service Provider agrees, acknowledges, represents and warrants as follows:

4.1 The Agreement permits Service Provider access to Confidential Information.
4.2 Service Provider shall hold the confidential information in strict confidence and access it only for the explicit business purpose of the Agreement.
4.3 Service Provider shall ensure compliance with the confidentiality and security conditions of the Agreement, Service Provider Safeguards Report and Service Provider Requirements and, as applicable, the GLBA and Safeguards Rule.
4.4 Service Provider shall protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own and its customers’ confidential information.
4.5 The University may require the prompt return or destruction of all copies of confidential information received by Service Provider upon completion of the Agreement.
4.6 Service Provider stipulates to allowing the entry of injunctive relief without the posting of bond in order to prevent or remedy breach of the confidentiality obligations of the Agreement.
4.7 Service Provider stipulates that any violation of the Service Provider Requirements shall constitute a material breach of the Agreement and entitles Temple University to immediately terminate the Agreement without penalty to Temple University.
4.8 Service Provider shall maintain controls to ensure that any subservicer used by Service Provider will also be able to protect and will protect customer information.
4.9 The University may request copies of audits and test result information that indicate the degree to which Service Provider and any subservicers implement appropriate information security measures.
4.10 The University may audit Service Provider’s compliance with Service Provider Requirements and Service Provider shall cooperate with the University in any such audits.
4.11 Service Provider Requirements shall survive any termination of the Agreement.

5. **Equitable Relief**

Service Provider acknowledges that a breach of the covenants in the Service Provider Requirements by Service Provider will result in irreparable and continuing damage to Temple University for which there will be no adequate remedy at law. Accordingly, in the event of any such breach, Temple University shall be entitled to injunctive relief and an order for specific performance with respect to such breach. Service Provider shall not oppose such relief on the grounds that there is an adequate remedy at law, and such right shall be cumulative and in addition to any other remedies at law or in equity (including, without limitation, monetary damages), which Temple University may have.