University Policies and Procedures

06-15.00 - IDENTITY THEFT POLICY

I. **Policy Statement:** Certain activities of Towson University (“University”) are subject to the provisions of the Federal Fair and Accurate Credit Transaction Act and the Federal Trade Commission’s Red Flag Rules. Under the Red Flag Rules, the University is required to establish an “Identity Theft Program” to detect, prevent and mitigate identity theft.

II. **Definitions:**

A. **Identity Theft:** a fraud committed or attempted using the Identifying Information of another person without authority.

B. **Red Flag:** a pattern, practice or specific activity that could indicate Identity Theft.

C. **Covered Accounts:** any account the University offers or maintains for which there is a reasonably foreseeable risk to Customers from Identity Theft, including those that involve multiple payments or transactions.

D. **Credit:** the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment on the purchase.

E. **Creditor:** an entity that regularly extends, renews, or continues Credit.

F. **Customer:** any person with a Covered Account.

G. **Identifying Information:** any name or number that may be used, alone or with other information, to identify a person, including name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, credit card number, unique electronic identification number, computer Internet Protocol address or routing code.

H. **Red Flag Rules Identity Theft Prevention Program** (the “Program”): the administrative, technical, or physical safeguards the University uses to identify, detect, prevent and mitigate instances of Identity Theft, as
required under the Federal Trade Commission’s FACT Act and the Red Flag Rule regulations.

I. Custodian: any University department, unit, or individual that administers Covered Accounts. Custodians will be identified in Appendix II and may be amended from time to time without the need to amend this policy.

J. Identity Theft Program Administrator: the individual responsible for developing, implementing, and updating the Program – the Associate Vice President for Financial Affairs.

III. Responsible Executive and Office:

   Responsible Executive: Vice President for Administration and Finance and Chief Fiscal Officer

   Responsible Office: Financial Affairs

IV. Entities Affected by this Policy: All divisions, colleges, departments and operating units.

V. The Program

   A. Towson University has established a Red Flag Rules Identity Theft Prevention Program to detect, prevent, and mitigate Identity Theft. The Program includes reasonable policies and procedures to:

      1. identify relevant Red Flags for Covered Accounts it offers or maintains and incorporate those Red Flags into the program;
      2. detect Red Flags that have been developed into the Program;
      3. respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
      4. ensure the Program is updated periodically to reflect changes in risks to Customers and to the safety and soundness of the Creditor from Identity Theft.

      5. The Program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

   B. The Program is included in Appendix I. The Program may be amended from time to time without the need to amend this policy.

VI. Responsibilities

   A. Employees who work with Covered Accounts must:
1. Complete University provided identity theft training.

2. Perform the day-to-day application of the Red Flags Rule Procedures to Covered Accounts by detecting and responding to red flags, as described in Appendix, sections B, C and D.

3. Under the Program, employees have a responsibility to obtain and verify the identity of persons opening or using Covered Accounts.

4. Employees are expected to notify their supervisor, the Program Administrator, and Management Advisory and Compliance Services if they become aware of an incident of identity theft or of failure to comply with the program.

B. Department Heads who supervise Employees who work with Covered Accounts must:

1. At least annually or as otherwise requested by the Program Administrator, staff responsible for compliance with the Program shall report to the Program Administrator on compliance with the Program.

2. Report incidents of Identity Theft or noncompliance with the Program to persons specified in the Program.

3. Maintain relevant records and make them available for review, including:
   a. department specific Red Flags Rule Procedures;
   b. documentation on training, including name, title, and date;
   c. documentation on instances of and attempts at Identity Theft;
   d. contracts with service providers that perform activities related to Covered Accounts;
   e. annually review the departmental Red Flags Rule Procedures to identify new Covered Accounts, changes to existing Covered Accounts, and changes in procedures for detecting, mitigating, and preventing identity theft. Maintain documentation of the annual review.

C. Identity Theft Program Administrator must:

1. Implement the Red Flags Identity Theft Prevention Program.

2. Periodically evaluate the Program considering incidents of and
attempts at Identity Theft, and update to reflect the current threat environment.

3. Take necessary corrective action if it is determined that a department is not adequately guarding against threats of Identity Theft.

4. Ascertain that service provider agreements are monitored so that, where applicable, such providers have adequate Identity Theft prevention programs in place.

5. Retain records relevant to the Program, including:
   a. Red Flags Identify Theft Prevention Policy;
   b. documentation on instances of Identity Theft and attempted Identity Theft.


8. Allow auditors and compliance officers access to the records.

VII. Enforcement

Individuals who have responsibilities as set forth in Section VI must: a) respect the confidentiality and privacy of individuals whose records they access; b) observe any restrictions that apply to sensitive data; and c) abide by applicable laws, policies, procedures, and guidelines with respect to access, use, or disclosure of information.

All faculty and staff who become aware of potential Identity Theft must report such an incident per the procedures defined by the Identity Theft Prevention Program Administrator. The Program Administrator will report violations to the appropriate entity. Violations of this policy may result in loss of usage privileges, administrative sanctions (including termination or expulsion) as well as personal civil and/or criminal liability.

Related Policies: USM Policy (VI – 10.00)

Approval Date: 10/14/2009
Effective Date: 10/14/2009
Amended Date: 3/8/2017

06-15.00 - 4
Approved by: President’s Council 07/30/2009
APPENDIX I
Identity Theft Program

A. As required by federal law, the University’s Identity Theft Prevention Program has the following four components:
   1. identification of relevant “Red Flags” and incorporation of them into the Program;
   2. detection of Red Flags that the Program incorporates;
   3. prevention and mitigation of Identity Theft by responding appropriately to detected Red Flags; and
   4. evaluation and adjustment of the Program periodically to reflect changes in risks, including periodic evaluation and adjustment of the Program based upon the results of testing and monitoring as well as changes in operations or operating systems.

B. Identification of Red Flags (Phase I)

To identify Red Flags, the University considers the types of Covered Accounts it offers and maintains the methods and business practices it provides to open, maintain, monitor and access such Covered Accounts and its previous experience with Identity Theft. The following are possible types of Red Flags for which employees working with Covered Accounts should receive program training, monitor appropriately, identify and resolve when possible, and refer, if necessary, to the Program Administrator for further resolution:

1. Notifications and warnings from Credit reporting agencies including:
   a. report of fraud accompanying a Credit report;
   b. notice or report from a Credit agency of a Credit freeze on a Customer or applicant;
   c. notice or report from a Credit agency of an active duty alert for an applicant; and
   d. indication from a Credit report of activity that is inconsistent with a Customer’s usual pattern or activity.

2. Suspicious Documents:
   a. identification document or card that appears to be forged, altered or inauthentic;
   b. identification document or card on which a person’s photograph or physical description is not consistent with the person presenting document;
   c. other document with information that is not consistent with existing information (e.g. an apparent forged signature); and

06-15.00 - 6
d. application for service that appears altered or forged.

3. Suspicious Personal Identifying Information:
   a. Identifying Information presented that is inconsistent with other information provided (e.g. inconsistent birth date);
   b. Identifying Information presented that is inconsistent with other sources of information (e.g. an address not matching an address on Credit report);
   c. Identifying Information presented that is the same information shown on other applications found to be fraudulent;
   d. Identifying Information presented that is consistent with fraudulent activity (e.g. an invalid phone number or fictitious billing address);
   e. social security number presented that is the same as one given by another Customer;
   f. an address or phone number that is the same as that of another;
   g. failure to provide complete personal Identifying Information (by law social security numbers must not be required); and
   h. Identifying Information inconsistent with the information on file.

4. Suspicious Account Activity:
   a. change of address for an account followed by a request to change the account holder’s name;
   b. payments stopped on a consistently up-to-date account;
   c. account used inconsistently with prior use (e.g. a significant change in how the account is used);
   d. an inactive account that is suddenly activated;
   e. mail to Customer is repeatedly returned as undeliverable while account is in use;
   f. notice to the University that Customer is not receiving mail about an account;
   g. notice that an account has unauthorized activity; and
   h. breach in University’s computer system security.

5. Notice from Others:
   a. Notice to the University that an account has been opened or used fraudulently.

C. Detection of Red Flags

1. New Accounts

   06-15.00 - 7
To detect Red Flags, each business unit working with new Covered Accounts will take appropriate measures, when possible, to verify the identity of a person opening a new account: This includes:

a. require Identifying Information such as name, date of birth, TU PeopleSoft ID number, residential or business address, or other identification used as part of University systems; and,

b. verify the Customer’s identity with photo identification (e.g. review a valid driver’s license or other identification card, such as OneCard, valid passport, permanent residence card, employment authorization card);

2. Existing Accounts

To detect Red Flags, each business unit working with existing Covered Accounts, will take appropriate measures when possible, to appropriately monitor transactions and verify identity when necessary:

a. verify the identification of Customers if they request information either in person, by telephone, facsimile or email;

b. verify the validity of requests to change billing addresses; and,

c. verify changes in banking information given for billing and payment purposes.

D. Responding to Red Flags and Mitigating Identity Theft

In the event University personnel detect Red Flags, such personnel shall take appropriate steps using current internal controls to respond and resolve Identity Theft depending on the nature and degree of risk posed by the Red Flag, including, but not limited to, the following:

1. continue to monitor an account for evidence of Identity Theft;

2. contact the Customer;

3. notify Program Administrator;

4. change any passwords or other security devices that permit access to accounts;

5. not open a new account;

6. close an existing account;

7. reopen an account with a new number; or

8. notify appropriate law enforcement and other University officials as appropriate, including Management Advisory and Compliance Services.

E. Best Practices

06-15.00 - 8
1. Best practices for securing documents and data, verifying identity, and monitoring service provider compliance are outlined below.

2. Best practices for paper documents:

File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive data must be locked when not in use. Storage rooms containing documents with sensitive data and record retention areas must be locked at the end of each workday or when unsupervised. Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing sensitive data when not in use. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas containing personal identifying information must be erased, removed, or shredded when not in use. University records may only be destroyed in accordance with the University’s records retention policy and applicable law. Documents containing personal identifying information must be destroyed in a secure manner such as via document shredding.

3. Best practices for electronic documents and data:

Personal identifying information in an electronic format must be protected from unauthorized access or disclosure at all times and may only be transmitted using approved methods including encryption as required using a University approved encryption program.

4. Best practices for identity verification:

Before an individual may open an account, his/her identity must be verified to determine if s/he is actually the person s/he claims to be. Similarly, before an individual may access or be provided with information concerning an existing account, s/he must demonstrate that s/he is authorized to access the account. Be sure to consider the different ways that an account-holder interacts with the school or department regarding their new or existing account including in-person, via phone, mail, or email, or online through a system. For opening a new account check a current government-issued identification card, like a driver’s license or passport. Depending on the circumstances, it may be prudent to compare that information with information available from other sources, like a credit reporting company or data broker, the Social Security Number Death Master File, or publicly available information. Asking challenge questions based on information from other sources can be another way of
verifying someone’s identity. For existing accounts an account holder may be asked to enter previously established confidential passwords and PIN numbers online to verify his/her identity and gain access to his/her existing account. For higher-risk situations, multi-factor authentication techniques including using passwords, PIN numbers, smart cards, tokens, and biometric identification are recommended. The University will never ask account holders to share their password or PIN with anyone else. Certain types of personal information – like a Social Security number, date of birth, mother’s maiden name, or mailing address – are not good authenticators because they are so easily accessible.

5. Best practices for service provider compliance:

Service providers that handle University accounts covered by the Red Flags Rule must comply with the regulation. A provision in the University’s contract with the service provider that requires them to have compliant policies and procedures in place will obligate the service provider to meet University Red Flags Rule standards. Service provider performance relative to identity theft prevention procedures can be monitored by the school or department by conducting an annual assessment of the service provider’s policies and procedures and by requiring reports from the service provider about incidents detected and their responses.

F. Program Oversight

1. Oversight of the Program will be assigned and shall include:
   a. assignment of specific responsibility to a Program Administrator for the implementation of the program;
   b. staff training and program materials; monitoring; compliance reporting and review;
   c. approval of material changes to the Program.

2. Reports shall be provided, at least annually, to the Responsible Executive. Reports will be prepared by staff/departments responsible for their particular administration of the Program and will include:
   a. the effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts;
   b. service provider agreements;
   c. significant incidents involving Identity Theft and management’s response; and
   d. recommendation for material changes to the Program.
G. Oversight of Service Provider Agreements

The University shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft whenever a service provider is engaged to perform an activity in connection with one or more Covered Accounts.
APPENDIX II
Custodians

A. The following areas are designated as Custodians of Covered Accounts including identifying information. This list will be updated with changes in the University’s Covered Account activity.

B. Custodian Departments and Programs

1. Registrar
2. Admissions
3. Financial Aid
4. Payroll
5. Human Resources
6. Public Safety
7. Accounts Payable
8. Health Services/Counseling
9. Procurement
10. Bursar’s Office
11. ID Card Office
12. Perkins Loan Program
13. DIAR installment payments
14. Auxiliary Services Business Office
15. Wellness Center
16. Athletics