TOURO UNIVERSITY WORLDWIDE AND TOURO COLLEGE LOS ANGELES
IDENTITY THEFT PREVENTION POLICY

1.0 POLICY/PROCEDURE

Touro adopts this identity theft policy to help protect employees, students, contractors and Touro from damages related to the loss or misuse of sensitive information that Touro classifies as "restricted" in its Information Security Policy.

2.0 PURPOSE

The risk to Touro, its employees and students from identity theft is of significant concern to Touro and may be reduced only through the combined efforts of every employee and contractor.

This Identity Theft policy will:

- Identify types of restricted information;
- Describe the physical security of restricted data when it is printed on paper;
- Describe the electronic security of restricted data when stored and distributed; and
- Place Touro in compliance with state and federal laws regarding identity theft protection.

This policy will also enable Touro to protect existing students, reduce risk from identity fraud, and minimize potential damage to Touro from fraudulent new accounts. The protection program put in place as a result of this policy will help Touro:

- Identify risks that signify potentially fraudulent activity within new or existing "covered accounts" (the definition of covered accounts is made in section 5 below);
- Detect risks when they occur in covered accounts;
- Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
- Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

3.0 SCOPE

This policy and protection program applies to all Touro employees, contractors, consultants, temporary workers, and other workers at Touro, including all personnel affiliated with third parties.

4.0 PROCEDURES

Restricted information (as repeated from the Information Security Policy) is information for which there are legal requirements preventing disclosure or financial penalties for disclosure. Data covered by federal and state legislation, such as FERPA or HIPAA, are in this class. Payroll and personnel information are also in this class because of privacy requirements. This Identity Theft Policy recognizes that other data may need to be treated as restricted to be in compliance with

Identity Theft Laws, and, as such, attempts to further identify the type of data that Touro handles that may be considered restricted.

4.1 Identification of Restricted Information

Restricted information includes the following items whether stored in electronic or printed format:

Credit card information, including any of the following:

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address

Tax identification numbers, including:

1. Social Security number
2. Employer identification numbers

Payroll information, including, among other information:

1. Paychecks
2. Pay stubs

Flexible benefits plan check requests and associated paperwork

Medical information for any employee or student, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information, e.g., patient names

Other personal information belonging to any student, employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Student Number

If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. If further clarification is required, the Dean or Provost of Touro will seek to clarify the information.

4.2 Hard Copy Distribution

Each employee and contractor performing work for Touro will comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with restricted information will be locked when not in use.

2. Storage rooms containing documents with restricted information and record retention areas will be locked at the end of each workday or when unsupervised.

3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing restricted information when not in use.

4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

5. When documents containing restricted information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*"

4.3 Electronic Distribution

Touro regulates electronic distribution of restricted information under the Touro Information Security Policy and Acceptable Use Policy.

Each Touro employee and contractor performing work for Touro shall comply with Touro policy guidelines that require:

1. Restricted information may only be transmitted internally, using approved internal e-mail via a wired connection to a Touro networked workstation. All restricted information must be encrypted when stored in an electronic format.

2. Restricted information in an electronic format must be protected from unauthorized access or disclosure at all times. Restricted information may not be sent externally unless encrypted and password protected and sent only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

"This email message and any attachments transmitted from Touro may contain confidential and legally protected information. If you are not the addressee and an intended recipient, you do not have permission to read, copy, use or disclose this email message and any attachments transmitted with this email to others; please notify the sender by replying to this message, and then delete it from your system."

4.4 Application of Other Laws and Touro Policies

Touro personnel must make reasonable efforts to secure Restricted and Confidential Information to the proper extent. Furthermore, this section should be read and applied in

conjunction with the Family Education Rights and Privacy Act ("FERPA") and other applicable laws and Touro policies. If an employee is uncertain of the treatment of a particular piece of information, he/she should contact Touro's Dean or Provost in writing.

5.0 Additional Efforts

5.1 Covered Accounts

For the purpose of Touro's Identity Theft Prevention Policy and Program, a "covered account" includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing account maintained by Touro for its students, faculty, staff, and other constituents that meets the following criteria is covered by this Program:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of Touro from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5.2 Red Flags

The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

1. Alerts, notifications or warnings from a consumer reporting agency (including a fraud or an active duty alert);
2. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or student, such as:

1. A recent and significant increase in the volume of inquiries;
2. An unusual number of recently established credit relationships;
3. A material change in the use of credit, especially with respect to recently established credit relationships; or
4. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

6.0 RESPONDING TO RED FLAGS

Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

- Canceling the transaction;
- Notifying and cooperating with appropriate law enforcement;
- Determining the extent of liability of Touro; and
- Notifying the actual student that fraud has been attempted