| Policies of the University of North Texas System Administration | Chapter 04 |
|---|---|
| **04.306 Identity Theft Prevention** | **Fiscal Management** |

**Policy Statement**. The University of North Texas System Administration will develop, maintain and update an Identity Theft Prevention Program ("Program") to detect, prevent, and mitigate Identity Theft in accordance with the Federal Trade Commission's "Red Flags Rule" (16 CFR §681). The Federal Trade Commission ("FTC") requires certain entities to adopt a Program to help prevent identity theft. FTC regulations related to Identity Theft prevention are part of the Fair and Accurate Credit Transactions Act and are collectively known as the Red Flags Rule. In compliance with the Red Flags Rule, the System Administration's Program is designed to better assist System Administration units and departments in identifying someone who may try to use another individual's identity to gain access to covered accounts at the System Administration. The Program is designed to detect, prevent and mitigate Identity Theft in connection with the opening of a Covered Account or any existing Covered Account.

**Application of Policy**. This policy applies to all employees and to students, staff, clients or patients that have a Covered Account with the System Administration.

**Definitions**.

1. Account. "Account" means any continuing financial relationship between the System Administration and an account holder that permits the account holder to obtain a product or service from the System Administration. It may involve the extension of credit for the purchase of a product or service, or a deposit account.

2. Covered Account. "Covered Account" is any student, staff, client or patient account that allows payment to be deferred; permits multiple payments or transactions, such as a loan that is billed or payable monthly; or poses a reasonably foreseeable risk of identity theft to consumers or businesses. These include, but are not limited to:

    - Participation in Federal Perkins Loan Program
    - Student Emergency Loan Program
    - Payment plans and promissory notes for covered student accounts
    - Payment plans for covered employee accounts, such as parking permit or donations

3. Identity Theft. "Identity Theft" is a fraud committed or attempted using the identifying information of another person without authorization.

4. Information Resources. "Information Resources" are the procedures, equipment and software that are employed, designed, built, operated and maintained to collect,

record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

5. Information Security. "Information Security" is the protection of information and Information Resources from threats in order to ensure business continuity, minimize business risks, and maximize the ability of the System, System Administration and Institutions to meet their goals and objectives. Information Security ensures the confidentiality, integrity and availability of Information Resources and information.

6. Personally Identifiable Information. "Personally Identifiable Information" means any name or number that may be used, alone or in conjunction with other information, to identify an individual, including, but not limited to:

   - Name
   - Address
   - Telephone Number
   - Social Security Number
   - Date of Birth
   - Government Issued Driver's License Number or Identification Number
   - Alien Registration Number
   - Government Passport Number
   - Employer or Taxpayer Identification Number
   - Unique Electronic Identification Number
   - Computer's Internet Protocol Address or Routing Code
   - UNT Assigned Student Identification Number

7. Red Flag. A "Red Flag" means a suspicious pattern, practice or specific activity that indicates the possibility of Identity Theft and that occurs in connection with a Covered Account at the System Administration.

**Procedures and Responsibilities.**

1. The Vice Chancellor for Finance shall establish, maintain and regularly update a written Identity Theft Prevention Program that is in compliance with the FTC's Red Flags Rule. The Program must:

   - Identify Covered Accounts.
   - Take into consideration the System Administration's previous Identity Theft experiences.
   - Take into consideration the methods the System Administration uses to open Accounts and provide access to them.

   Responsible Party: Vice Chancellor for Finance

2. The Vice Chancellor for Finance is responsible for oversight of the System Administration's Program. The Associate Vice Chancellor for Finance and Administration is designated as the Program Administrator for the Program and is responsible for developing, implementing, maintaining and day-to-day operation of the Program. The Program Administrator or designee works with departmental or unit administrators in areas affected by the Red Flags Rule to ensure understanding and compliance with the Program. The Program Administrator or designee also works in conjunction with the System's Information Security Officer to address Red Flags and Identity Theft issues related to Information Resources and Information Security.

   Responsible Party: Vice Chancellor for Finance and Associate Vice Chancellor for Finance and Administration

3. System Administration departments or units are required to conduct periodic risk assessments to determine if the department or unit has responsibility for Covered Accounts, which should be recognized by and added to the Program.

   Responsible Party: Heads of departments or units

4. Departmental or unit administrators in areas affected by the Red Flags Rule are responsible for ensuring compliance with the System Administration's Program in their department or unit.

   Responsible Party: Heads of departments or units affected by the Red Flags Rule and departmental or unit administrators in areas affected by the Red Flags Rule

5. The Program Administrator or designee shall work in conjunction with the System's Information Security Officer to provide Identity Theft prevention training as needed to ensure understanding of and compliance with the Program by departmental or unit administrators in areas affected by the Red Flags Rule.

   Responsible Party: Associate Vice Chancellor for Finance and Administration

6. At least annually before the end of the fiscal year, departments and units that maintain Covered Accounts are required to make an identity theft prevention report to the Program Administrator in accordance with reporting requirements set forth in the written Program.

   Responsible Party: Heads of departments or units in areas affected by the Red Flags Rule

7. The Program Administrator is responsible for conducting an annual Program assessment and providing an annual report to the Vice Chancellor for Finance.

   Responsible Party: Associate Vice Chancellor for Finance and Administration

8. The Program will be reviewed annually by the Program Administrator in accordance with the review requirements set forth in the written Program. The annual review will include input from the System's Information Security Officer and the System Administration's Information Security Officer. After the risk assessment is conducted, the Program Administrator will recommend updates to the Identity Theft Prevention Policy and Program. The Vice Chancellor for Finance will authorize updates as necessary, after any policy revisions have been approved by the Chancellor in accordance with the standard process for revising policies.

   Responsible Party: The Chancellor, the Vice Chancellor for Finance, and the Associate Vice Chancellor for Finance and Administration

**References and Cross-references**.

16 Code of Federal Regulations §681
University of North Texas System Regents Rule 10.800

**Forms and Tools**

UNT System Administration Identity Theft Prevention Program
UNT System Information Security Handbook

Approved: October 4, 2017
Effective: October 4, 2017
Revised: