POLICY TITLE: Identity Theft Prevention

POLICY PURPOSE: The purpose of this statement is to set forth Fort Hays State University policy with regard to the detection, prevention, and mitigation of identity theft in connection with various accounts maintained by the University. The Federal Trade Commission's "Red Flags Rule" implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This policy is intended to implement an Identity Theft Prevention Program for the University that:

- Identifies relevant warnings ("Red Flags") for certain identified covered accounts it offers or maintains;
- Detects those Red Flags that have been identified;
- Responds appropriately to any Red Flags that are detected to seek to prevent and mitigate identify theft;
- Ensures that the Identity Theft Prevention Program is reviewed periodically and updated as appropriate to reflect changes in risks to students and with regard to the safety and soundness of credits from identity theft; and
- Encourages University employees to report suspected cases of identity theft involving a covered account or student to the Vice President of Administration and Finance or to the University General Counsel's office.

BACKGROUND:

APPLIES TO: Everyone

DEFINITIONS: "Identity Theft" is a fraudulent or attempted use of identifying information of another person without such person's authority.

A "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

"Covered Account" is an account that is offered or maintained to permit multiple payment transactions for business, personal, family and household purposes for which there is a reasonably foreseeable risk of identity theft. For purposes of this program, examples of covered accounts maintained or offered by FHSU include but are not limited to:

- Student tuition and fee payment plans;

- Residential Life payment plans (room and board);
- Financial Assistance programs and repayment plans associated therewith, when applicable;
- Federal Perkins Loans;
- FHSU Institutional Loans, and;
- Any other account the University offers or maintains for which there is a reasonably foreseeable risk to consumers or to the safety and soundness of the University from Identity Theft.

"Consumer" means any person with a Covered Account with the University.

“Identifying Information” means any name or number that may be used alone or in conjunction with any other information, to identify a specific 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
- Employer or taxpayer identification number
- Unique electronic identification number
- Computer’s Internet Protocol address or routing code

“Service Provider” means a person that provides a service directly to the University.

CONTENTS:

POLICY STATEMENT:

Identification of Relevant Red Flags

The University Identity Theft Program identifies the following Red Flags:

- Documents provided for identification appear to have been altered or forged;
- The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
- A request made from a non-FHSU issued email account;
- A request to mail something to an address not listed on file; or
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Examples of Red Flags

- Alerts, notifications or warnings from a consumer reporting agency

including a fraud alert in connection with a consumer report;
- A notice of address discrepancy received from a consumer reporting agency;
- A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity on that account;
- Suspicious documents including: documents used for identification that appear to have been altered or forged; and photographs or physical descriptions on an identification that are inconsistent with the appearance of the applicant or customer presenting the identification, or other inconsistent information on the identification;
- Suspicious personal identifying information including: personal identifying information provided by the customer not consistent with other personal identifying information; personal identifying information that is of the type commonly associated with fraudulent activity as indicated by internal or third-party sources, such as a fictitious address or a social security number that matches a social security number provided by another customer; and personal identifying information that is not consistent with other information on file with the University;
- Unusual or suspicious activity related to the covered account, including but not limited to notice to the University that a student is not receiving mail sent by the University, a breach of the University's computer system security, and unauthorized access to or use of student account information, and;
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identify theft in connection with covered accounts held by the University.

Detecting Red Flags

In order to attempt to detect Red Flags, the University will obtain identifying information about the person opening a covered account and attempt to verify such person's identity to the extent reasonable and possible, by comparing the information received with other information on the same person maintained by the University. In addition, the University may take one or more of the following actions to detect Red Flags:

- Require certain identifying information such as name, date of birth, academic records, home address or other identification, including verification of student's identity through photo identification for issuance of the student identification card (Tiger Card);
- Verify identification of students if they request information or changes in banking information given for billing and payment purposes;
- Require written verification that an address is accurate at the time the credit report request is made to the consumer reporting agency, and in the event there is an address discrepancy, verify that the report pertains to the applicant for whom the report was requested;
- Monitor account when specific activity on that activity occurs.

Responding to Red Flags

When the University has detected a possible Red Flag associated with a covered account, the administrator of the Program may take one or more of the following actions:

- Contact the customer to verify inconsistent information or to verify recent activity on the account;
- Monitor the covered account for unusual or suspicious activity;
- Change any password, security code or other security device that permit access to a covered account;
- Close an existing covered account;
- Notify law enforcement when circumstances indicate possible criminal activity;
- Determine that no particular response is warranted under the circumstances presented; and
- Post a notification to the campus community of the suspected incident involving identity theft on the University's Police Department website.

Updating the Program

The University will review the program periodically, and no less than once per year, to determine whether updates and modifications are needed based upon experience with identifying and responding to Red Flags. Also, the program will be reviewed and updated if the University becomes aware of changes in methods of committing, preventing and/or detecting identity theft. Finally, changes in the type or nature of accounts that the University maintains and particular business arrangements of the University may require an update to the program.

Oversight of the Identity Theft Prevention and Periodic Review

Overall responsibility for developing and implementing the Identity Theft Prevention Program lies with the Vice President of Administration and Finance or the Vice President's designee. The Vice President of Administration and Finance or the Vice President's designee will implement and facilitate an annual review of the University Identity Theft Prevention Program and suggest updates as deemed appropriate or as required by law.

Oversight of Service Provider Relationships

The Vice President for Administration and Finance or designee shall also be responsible for oversight of service provider arrangements. 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 the University engages a service provider to perform an activity in connection with one or more covered accounts.

Staff Training

	University employees responsible for implementing the Identity Theft Prevent Program shall be trained in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. Training shall be provided on an annual basis.
EXCLUSIONS OR SPECIAL CIRCUMSTANCES:	
RELATED DOCUMENTS:	**Policies:** **Forms:** **Other:**
KEYWORDS:	Identity theft, Federal Trade Commission, red flag, suspicious activity
RESPONSIBLE OFFICE:	Administration and Finance
RESPONSIBLE UNIVERSITY OFFICIAL:	Vice President for Administration and Finance
ORIGINATION DATE:	6/17/09
REVIEW CYCLE:	Every year

POLICY ADDRESS:	
LAST APPROVED ON:	Adopted by President's Cabinet 11/28/2018
REVIEW/CHANGE HISTORY:	Adopted by President's Cabinet 6/17/09
NEXT REVIEW DATE:	10/2019
