SOFIA UNIVERSITY

Identity Theft Prevention Program

Derived from the FTC Red Flags Rule requirements

1.0 Introduction

In 2003, Congress enacted the Fair and Accurate Credit Transactions Act of 2003, 15 U.S.C. Section 1681, et seq. ("FACTS ACT"), which requires "creditors" to adopt policies and procedures to prevent identity theft. The Federal Trade Commission ("FTC") has promulgated 16 C.F.R. Section 681.1, commonly known as the "Red Flags Rule," pursuant to its authority under the FACTS ACT. After consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities, the University determined that this policy was appropriate and necessary for University compliance.

Under the Red Flags Rule, every financial institution and creditor is required to establish an Identity Theft Prevention Program tailored to the size, complexity, and nature of its operation. Sofia University is considered a financial institution and a creditor under the rules since it receives federal grants and allows for the delay of payments for its services.

In short, a "red flag" is an event that should alert an organization to a potential risk of identity theft. To comply with the Red Flags Rule, Sofia University must develop an Identity Theft Prevention program that clearly defines procedures to aid in the identification, detection, and governs the response to potential identity theft red flags.

Additional information on the rules and how they apply to Sofia University may be found at: http://www.ftc.gov/redflagsrule

2.0 Purpose of this Plan

This policy and procedure is intended to help protect students, faculty, staff, and other constituents and the University from damages related to the fraudulent activity of identity theft. It is not intended to specify all the details of the Program or identify all possible instances for identity theft. This policy and procedure requires departments to maintain written procedures, identify specific "Red Flags," outline appropriate responses to "Red Flags" that are detected to mitigate identity theft, and establishes recommended employee training.

3.0 Scope

Sofia University is committed to supporting the intent of the Red Flags Rule and to protecting the privacy of the University and its constituents. As such, every department of the University is required to comply with this plan in its procedures and policies. Each University entity with access to personal identification and financial information is required to develop and implement reasonable internal written procedures to comply with the Red Flags Rules as well as other privacy requirements (e.g.; Gramm-Leach-Bliley, FERPA, HIPAA etc.).

4.0 Definitions as Defined in the FACTS ACT and the Red Flags Rule

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

B. "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

C. "Creditor" is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan program
- Participation as a school lender in the Federal Family Education Loan Program
- Offering institutional loans to students, faculty or staff
- Offering a plan for payment of tuition or fees throughout the academic terms, rather than requiring full payment at the beginning of the term

D. "Covered Account" includes all bursar accounts or loans that are administered by the University. Additionally, it includes any other account for which there is a reasonably foreseeable risk of identity theft.

E. "Program Administrator" is the individual designated with primary responsibility for oversight of the Program. See Section 9.01.

F. "Identifying Information" is "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, student identification number, computer's Internet Protocol address, or routing code.

5.0 Red Flags

The University identifies the following Red Flags in addition to any specific flags identified within departmental policies:

1) Notifications and Warnings from Credit Reporting Agencies
    a) Red Flags
        i) Report of fraud accompanying a consumer/credit report
        ii) Notice or report from a credit agency of a credit freeze
        iii) Notice or report from a credit agency of an active duty alert for an applicant
        iv) Receipt of a notice of address discrepancy in response to a consumer/credit report request

v) Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity. For example:
   (1) recent significant increase in the volume of inquiries
   (2) an unusual number of recently established credit relationships
   (3) material change in the use of credit, especially with respect to recently established credit relationships
   (4) account that was closed for cause or identified for abuse of account privileges by the University

2) Suspicious Documents
   a) Red Flags
      i) Identification document or card that appears to be forged, altered, or inauthentic
      ii) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
      iii) Other document with information that is not consistent with existing account holder/student information
      iv) Other information on the provided is inconsistent with readily available information on file with the University
      v) Application for service that appears to have been altered or forged

3) Suspicious Personal Identifying Information
   a) Red Flags
      i) Identifying information presented that is inconsistent with other information the account holder/student provides. For example:
         (1) Inconsistent birthdate
         (2) Address does not match any address in the consumer report
         (3) The Social Security Number has not been issued or is listed on the Social Security Administration's Death Master File.
      ii) Identifying information presented that is inconsistent with other sources of information. For example:
         (1) permanent address does not match the permanent address on a loan application
         (2) The phone number on an application is the same as the number provided on a fraudulent application
      iii) Identifying information presented that is the same as information shown on other documents that were found to be fraudulent
      iv) Identifying information presented that is consistent with fraudulent activity. For example:
         (1) The address on an application is fictitious, a mail drop, or a prison
         (2) The phone number is invalid or associated with a pager or answering service
      v) Social security number presented that is the same as one given by another account holder/student
      vi) A person fails to provide complete personal identifying information on a document when reminded to do so

vii) A person's identifying information is not consistent with information that is on file for the account holder/student.

viii) For departments or groups using a "challenge question" to identify an account holder, the person opening the account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report

4) Suspicious Covered Account Activity or Unusual Use of Account
   a) Red Flags
      i) Change of address for an account followed by a request to change the account holder/student's name or other information
      ii) Account used in a way that is not consistent with prior use. For example:
         (1) The majority of available credit is used for cash advances or merchandise that is easily convertible to cash
         (2) The person fails to make the first payment or makes an initial payment but no subsequent payments
         (3) Nonpayment when there is no history of late or missed payments
         (4) An increase in the use of available credit
         (5) Change in spending patterns
         (6) Change in electronic fund transfer patterns in connection with a deposit account
         (7) Change in telephone call patterns in connection with a cellular phone account
      iii) Mail sent to the account holder/student is repeatedly returned as undeliverable
      iv) Notice to the University that an account holder/student is not receiving mail sent by the University
      v) Notice to the University that an account has unauthorized activity
      vi) Breach in the University's computer or network security
      vii) Unauthorized access to or use of account holder/student account information
5) Alerts from Others
   a) Red Flags
      i) Notice to the University by an account holder/student, identity theft victim, law enforcement, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft

6.0 Detecting Red Flags

A. Student Enrollment - In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account (individual departmental policies may contain additional Red Flags specific to their area):

1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and

2. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government issued or tribally issued photo identification).

B. Existing Accounts - In order to detect any of the Red Flags identified above for an existing covered account, University personnel will take the following steps to monitor transactions on an account (individual departmental policies may contain additional verifications specific to their area):

1. Verify the identification of account holders/students if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing address by mail or email and provide the account holder/student a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests - In order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1.Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the application for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

7.0 Responding to Red Flags

In the event that University personnel detect any of the identified Red Flags or suspects Identity Theft, personnel shall first file a Notice of Suspected Privacy Breach (Appendix A) and take one or more of the following steps:

a. Decline to make any changes to the account, do not issue replacement ID cards, deny access to the account, or otherwise block the requested access.
b. Continue to monitor a covered account for evidence of identity theft
c. Contact the account holder/student or document provider
d. Change any passwords or other security devices that permit access to covered accounts
e. Not open a new covered account
f. Provide the account holder/student with a new campus identification number
g. Notify the Program Administrator for determination of the appropriate step(s) to take
h. Notify law enforcement

i. Notify the President, Chief Operating Officer, Chief Financial Officer, Registrar, Director of Human Resources, or utilize an anonymous reporting hotline provided by the University, if one is provided.
j. Determine that no additional response is warranted under the particular circumstances

8.0 Additional Measures to Prevent Misuse of Account Holder/Student Identifying Information

In order to mitigate the risk of identity theft with respect to all covered accounts, the University shall also take the following steps:

a. Ensure that all websites where personal information is inputted are secure by use of SSL certificates
b. Ensure the complete and secure destruction of paper documents and computer files containing account holder/student account information when a decision has been made to no longer maintain such information
c. Ensure that all employee computers that may access covered account information are password protected by use of an employee network account that may be disabled
d. Ensure that all employee computers that may access covered account information have password protected screen savers
e. Avoid use of social security numbers as identifiers where possible
f. Ensure that network and computer anti-virus protection is up-to-date
g. Keep only information that is necessary for University purposes

9.0 Program Administration

A. Oversight
   a. Responsibility for developing, implementing, and updating this program lies with the Chief Operating Officer who also serves as the Program Administrator. The program, changes, and enforcement are supported and reviewed by the President's Cabinet. Responsibility for training lies with the Chief Operating Officer and each department head within the University.
   b. Review of all reports lies with the Program Administrator.
B. Staff Training and Reporting
   a. All staff responsible for implementing the Program shall be trained by or under the direction of the Program Administrator.
   b. The staff responsible for implementing the Program is responsible for training others within their functional area.
   c. It is recommended that staff sign a document to be stored in their personnel file stating that they have been trained and understand this policy. (Appendix B)
C. Departmental Policies and Procedures
   a. Each department within the University is required to review and adhere to this program

b. All procedures and policies shall state compliance with this program and detail any additional red flags, mitigation steps, and procedures above and beyond those stated within this program

D. Service Providers to the University
    a. For all third-party service providers to the University who may come in to contact with information on covered accounts, the University will require:
        i. That the provider have similar policies and procedures in place to prevent identity theft
        ii. That the provider review the University's program and report any red flags to the Program Administrator or the agent of the University with primary oversight of the relationship

E. Program Updates
    a. Updates will be made to this program as necessary and will be reviewed by the President's Cabinet

SOFIA UNIVERSITY

Chief Operating Officer
1069 E. Meadow Cir.
Palo Alto, CA 94303
Phone: 650-388-5320

NOTIFICATION OF SUSPECTED PRIVACY BREACH

Name of person whose Privacy may have been breached:	*ID #:*
Email Address:	*Phone:*
Is the individual aware of the incident? **YES/NO** If **NO**, please do not inform the individual unless so instructed.	
Name of person making complaint (if different from above):	*Relationship*

Data Involved: ☐ Bursar ☐ Academic ☐ Other (*please describe*):
☐ Health ☐ Perkins Loan
☐ Personal ☐ Other

Date of Incident:_____

I feel that my / this person's privacy has been breached in the following way:

Harm or Negative Outcome:

Signature: _____ **Date:** _____

Return this form to Sofia University, Chief Operating Officer, 1069 E. Meadow Cir., Palo Alto, CA 94303 or email to Ryan.Haylock@sofia.edu. Please keep a copy for your records.

For Office Use Only:

Completed by (please print): _____ **Date:** _____

College/Department: _____ **Ext:** _____

Signature:_____

Action Taken:_____

_____