CLEAR ALL

UNIVERSITY OF CENTRAL FLORIDA

Identity Theft Prevention Program
Annual Assessment Worksheet
For Calendar Year: _____

UCF maintains an Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule ("Red Flags Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. UCF's program is outlined in University of Central Florida Identity Theft Prevention Policy 2-105.1.

This worksheet requests that you document your department/unit's compliance with the Red Flags Rule including:

- Clearly identifying and documenting covered accounts
- Establishing sources to identify red flags
- Identifying the controls to detect, prevent and mitigate identity theft
- Providing employee training
- Ensuring compliance by third party service providers

To complete this worksheet, you must have a thorough understanding of the university policy noted above. All units who have covered accounts must complete or update this worksheet at least annually. Once this worksheet is completed, it is considered a confidential document and is not for public disclosure. Employees who prepare the program or have access to it must take appropriate steps to ensure that the data therein is securely maintained. This document is subject to review and audit by University Audit and the Red Flags Committee.

A. Contact Information

1. Identify your department/unit: _____

2. Provide the contact information of the person responsible for administering the identity theft prevention program in your department/unit.

Contact Person:	
Title:	
Telephone:	
E-mail:	

3. Provide contact information for the person completing this worksheet, if different from the contact person listed above.

Name:	
Title:	
Telephone:	
E-mail:	

B. General Business Processes

1. The Identity Theft Prevention Policy applies to you if your unit engages in the following activities. Select the boxes next to any activities performed by your department/unit.

   ☐ Enter or alter personally identifying information in a university system or database.

   ☐ Maintain systems that generate personally identifying information.

   ☐ Offer goods or services that individuals can pay for later on an account administered by or on behalf of your office.

   ☐ Administer billing, declining balance, debit, or other accounts whether on behalf of your own unit or another university unit/department.

   ☐ Make loans, such as short-term loans to students, faculty, or staff.

   ☐ Administer student loans.

   ☐ Issue cards to individuals that can be used to access accounts.

   ☐ Use consumer credit reports such as those issued by Experian, TransUnion, or Equifax.

   ☐ Report information to credit reporting agencies.

   ☐ Bill for fines.

   ☐ Pursue debt collection.

   ☐ Offer leases to individuals for personal use/non-business purposes.

   ☐ Sell or transfer debts to a third party.

2. Have all employees who are responsible for following the department/unit's identity theft prevention program completed the online training course, *FSC 113: Red Flags-Identity Theft Prevention*? If not, please provide the date by when the training will be completed.

   Note: The F&A Red Flags Coordinator will provide a list of employees who have completed the online training upon request.

   ☐ Yes

   ☐ No → Date of Completion: _____

3. Describe any departmental training or identity theft prevention program materials provided to employees. If not applicable, enter N/A and skip to the next question.

   Note: Please attach any departmental training or awareness materials to this worksheet when you return it.

   _____

   _____

   _____

   _____

   _____

   _____

   _____

   _____

4. The following is a list of procedures used to protect personal information. Select the boxes next to any procedures used in your department.

   ☐ Web servers and database servers are securely maintained based on university standards.

   ☐ Computer workstations are protected based on university standards.

   ☐ Office computers with access to covered account information are password protected and comply with university identity and access standards.

   ☐ Record retention requirements are followed and documents and computer files containing personally identifiable information (PII) are securely destroyed when necessary.

   ☐ The Social Security Number (SSN) policy is followed and the use of SSN is avoided when appropriate.

   ☐ Information is not collected beyond what is necessary to satisfy the immediate business reason at hand.

C. Red Flags Background

1. Without identifying individuals, briefly describe the previous experience your department/unit has had with red flags. Indicate the frequency of occurrence over the last three years.

   _____

   _____

   _____

   _____

   _____

2. Did your unit report an identity theft incident this year? If so, when and to whom was it reported?

   ☐ Yes → Date: _____ Reported to: _____

   ☐ No

3. If you have become aware of new methods of identity theft in the past year, describe them and the impact on your department/unit's identity theft prevention program.

   _____

   _____

   _____

   _____

   _____

D. Covered Accounts

Certain types of accounts may be covered under the Red Flags Rule. Examples of covered accounts are as follows:

- Perkins loan program
- Institutional loans
- Student billing and receivables
- Student refunds
- Accounts in collection
- Short term loans/ advances
- UCF Card
- Dining, housing, parking payment plans

- Restitution accounts with installment payments
- Credit bureau data
- Student records

Covered accounts may be classified into one of the following two types. You need to understand these types to answer the questions in this section of the worksheet. Descriptions are as follows:

Type 1

An account you offer your customer that involves multiple transactions or payments in arrears. Common examples are loans and billing for previous services rendered. Type 1 covered accounts are always covered under the Red Flags Rule.

Type 2

Any other account for which personally identifiable information is maintained AND there is a reasonably foreseeable risk to customers or to the safety and soundness of the university, including financial, operational, compliance, reputation or litigation risks. This type of account is only covered under the Red Flags Rule if the risk of identity theft is reasonably foreseeable, thus requiring an assessment of risk.

1. List the Type 1 covered accounts that are established and/or accessed by your department/unit.
    a. _____
    b. _____
    c. _____
    d. _____
    e. _____
    f. _____
2. List the Type 2 covered accounts that are established or accessed by your department/unit.
    a. _____
    b. _____
    c. _____
    d. _____
    e. _____
    f. _____

3. Describe your department/unit's business process for establishing and accessing each type of covered account listed in #1 and #2.

Covered Account	Process for Establishing	Process for Accessing

4. List third-party service providers who are engaged by your department/unit to perform an activity in connection with a covered account in #1 or #2. Also, list the services they provide and the type of personally identifiable information (PII) maintained. Include university-related organizations and other direct support organizations (DSOs). Do not include other university departments.

Covered Account	Service Provider	Services Performed	PII

5. Answer the following questions if your department/unit processes enrollments or address/billing changes for existing accounts with regard to any type of covered account listed in #1 or #2.

   If not applicable, enter N/A here and skip to the next question: _____

   a. Do you receive and maintain PII (i.e. name, address, telephone number, date of birth, Social Security Number, etc.) about account holders?

      ☐ Yes

      ☐ No

   b. If you selected Yes for 5a, how are the enrollments and address/billing changes requested and processed? Check all that apply.

- ☐ In person
- ☐ Online or e-mail correspondence
- ☐ By telephone
- ☐ Mail correspondence
- ☐ Other: _____
- ☐ Not applicable

c. Do you require documentation and/or proof of identity for enrollments and address/billing changes for existing accounts?

- ☐ Yes
- ☐ No

d. If you selected Yes for 5c, what documents are required? Check all that apply.

- ☐ Driver's license
- ☐ UCF Card
- ☐ Social Security Card
- ☐ Other: _____
- ☐ Not applicable

e. What is the name of the software application in which personal information is maintained? If not applicable, enter N/A.

_____

f. If the account holder has the ability to log in and alter personal information, does the application send the account holder email notifications each time personal information (email address, physical address, banking information, SSN, etc.) is changed? If so, please describe any exceptions to the rule. If not applicable, enter N/A.

_____

_____

_____

_____

_____

6. Answer the following questions if your department/unit receives reports from consumer reporting agencies.

   If not applicable, enter N/A here and skip to the next question: _____

a. Describe your department/unit's policy to address discrepancies between information provided by the customer, the credit report and any other data (i.e. internal files, etc.).

_____

_____

_____

_____

_____

_____

b. Describe your department/unit's procedures and timelines for reporting verified addresses back to the reporting agency.

_____

_____

_____

_____

_____

_____

c. What is your department/unit's policy if you receive an alert, notification or warning from a consumer reporting agency? Check all that apply.

- ☐ Require additional documentation
- ☐ Compare with other information on file
- ☐ Suspend account
- ☐ Contact account holder
- ☐ Other: _____
- ☐ Other: _____

E. Identifying Red Flags

Red flags indicate the possible existence of identity theft. In this section, you will list the red flags applicable to the covered accounts in your unit, along with the controls that are used to prevent, detect, and respond to each relevant red flag.

Note: Attachment A contains a list of possible red flags identified by the Federal Trade Commission (FTC).

The preparer of this worksheet is expected to use Policy 2-105.1 as a guide for completing the following tables. The Policy identifies examples of red flags for each of the four categories below. Most units will have one or more relevant red flags in each category. Insert additional rows if necessary. Further instructions are included in the footnotes that follow the tables.

1. With your department/unit's covered accounts and business processes in mind, list any red flags you may encounter relating to **suspicious documents**. Examples of suspicious document red flags include but are not limited to:
    - An ID card or document that appears to be forged, altered, or inauthentic
    - An ID card or document on which a person's photograph or physical description is not consistent with the person presenting the document
    - Information on any document is not consistent with existing identifying information
    - An application for service that appears to have been altered or forged.

Relevant Red Flag[1]	Detection Mechanism[2]	Response Required[3]	Resolution[4]
Example - Documents provided for identification appear to have been forged, altered, or inauthentic	*Example - View and scrutinize documents provided*	*Example - Notify management; do not provide assistance*	*Example - Retain suspicious documentation; report to supervisor*

2. With your department/unit's covered accounts and business processes in mind, list any red flags you may encounter relating to **suspicious PII**. Examples of PII red flags include but are not limited to:
    - Identifying information presented that is inconsistent with other information provided (e.g., inconsistent birth dates)

- Identifying information presented that is inconsistent with other sources of information (e.g., an address doesn't match one provided on a loan application)
- PII provided matches PII identified as belonging to another person
- A person fails to provide complete PII on an application after being reminded to do so

Relevant Red Flag[1]	Detection Mechanism[2]	Response Required[3]	Resolution[4]
Example – SSN provided matches SSN of another person.	*Example – An error message stating that a record already exists is received when inputting customer information into the database*	*Example – Stop processing and inform management; escalate for investigation if necessary*	*Example – Delay processing until PII is confirmed as accurate, if applicable*

3. With your department/unit's covered accounts and business processes in mind, list any red flags you may encounter relating to **unusual use of, or suspicious activity related to, the covered account**. Examples of suspicious activity red flags include but are not limited to:
    - Payments stop on an otherwise up-to-date account
    - Account is used in a way that is not consistent with prior use
    - Mail sent to the individual is repeatedly returned as undeliverable
    - Breach in university's computer system security

Relevant Red Flag[1]	Detection Mechanism[2]	Response Required[3]	Resolution[4]
Example – Payments stop on an otherwise up-to-date account	*Example – Account holder appears on a report identifying account anomalies*	*Example – Customer is contacted and asked if they are aware of the overdue payments*	*Example – If account is valid, activity will resume when payments are up-to-date; if account is invalid, management will investigate further*

4. With your department/unit's covered accounts and business processes in mind, list any red flags you may encounter relating to **alerts from others**. Examples of alert-related red flags include but are not limited to:

    - Notifications and warnings from credit reporting agencies
    - Notice to the university from an individual, an identity theft victim, a law enforcement official or other person that the university has opened or is maintaining a fraudulent account

Relevant Red Flag[1]	Detection Mechanism[2]	Response Required[3]	Resolution[4]
Example – Notice from a credit agency of a credit freeze on an applicant	*Example – Review of credit agency notices*	*Example - Notify management; do not continue processing application*	*Example - Retain report with application; report to supervisor*

[1] Refer to Section II of Policy 2-105.1 for a list of possible red flags that have been identified by the university. Include all (even those not specifically listed in the policy) that apply to your covered account(s).

[2] Refer to Section III of Policy 2-105.1 for suggested detection mechanisms that have been identified by the university. Include all (even those not specifically listed in the policy) that are used to recognize a possible occurrence of identity theft with regard to your covered account(s).

[3] Refer to Section IV of Policy 2-105.1 for the red flag responses that have been identified by the university. Include all (even those not specifically listed in the policy) that are used to prevent and mitigate a possible occurrence of identity theft with regard to your department's covered account(s).

[4] Policy 2-105.1 requires university employees to notify University Audit once they become aware of an incident of identity theft or of the university's failure to comply with this program.

Click here to submit. Submission of this form is considered your digital signature.

Signature

_____

Date

ATTACHMENT A

Possible Red Flags Identified by the Federal Trade Commission (FTC)

The FTC has identified 26 possible red flags[1]. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point in their individual evaluations.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in §681.1(b) of the regulations.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

    a. A recent and significant increase in the volume of inquiries;

    b. An unusual number of recently established credit relationships;

    c. A material change in the use of credit, especially with respect to recently established credit relationships; or

    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information (PII)

10. PII provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

    a. The address does not match any address in the consumer report; or

    b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. PII provided by the customer is not consistent with other PII provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. PII provided is associated with known fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor. For example:

    a. The address on an application is the same as the address provided on a fraudulent application; or

    b. The phone number on an application is the same as the number provided on a fraudulent application.

13. PII provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

    a. The address on an application is fictitious, a mail drop, or a prison; or

    b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required PII on an application or in response to notification that the application is incomplete.

17. PII provided is not consistent with PII that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the Institution or creditor receives a request for a new, additional or replacement card; a cell phone, or the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:

    a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

    b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

    a. Nonpayment when there is no history of late or missed payments;

    b. A material increase in the use of available credit;

    c. A material change in purchasing or spending patterns;

    d. A material change in electronic fund transfer patterns in connection with a deposit account; or

    e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that has opened a fraudulent account for a person engaged in identity theft.

[1]"Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rule" 72 Federal Register 217 (9 November 2007), pp. 63755 – 63756.