Office of the President
University Policy

SUBJECT:	Effective Date:	Policy Number:
IDENTITY THEFT PREVENTION PROGRAM	6-17-09	5.6
	Supersedes:	**Page** **Of**
	New	**1** **7**
	Responsible Authority:	
	Senior Vice President, Finance & Administration	

APPLICABILITY/ACCOUNTABILITY:

This policy is applicable to all members of the university community, including all employees, contractors, consultants, temporary workers, and service providers, including all personnel affiliated with third parties.

POLICY STATEMENT:

I. Purpose

To establish an Identity Theft Prevention Program ("Program") designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide continued administration of the Program in compliance with 16 C.F.R. Part 681.

This Program enables Florida Atlantic University ("FAU" or "University") to protect existing

C. A *red flag* means a pattern, practice or specific activity that indicates the possible existence of identity theft.
D. *Personally identifiable information* includes the following items whether stored in electronic or printed format: first, middle, or last name, legal name, date of birth, addresses, telephone or wireless numbers, social security number, government-issued identification number, passport number, maiden name, account number, credit card information (number, expiration date, name, address), and emergency contact information.

III. The Program

FAU establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

A. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the Program;
B. Detect red flags that have been incorporated into the Program;
C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
D. Ensure the Program is updated periodically to reflect changes in risks to covered account holders.

IV. Administration of the Program

The FAU Office of Financial Affairs, with the assistance of the Office of the General Counsel, shall be responsible for the development, implementation, oversight and continued administration of the Program. Oversight responsibility of the Program is delegated to the Controller. Operational responsibility of the Program is delegated to the applicable supervising authorities for FAU colleges, departments or divisions reh223overed accoun.o:

IV. Identificati(y oR relevanRereF flaam)TJEMC ET10328.000186.42 of the Program

2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or account holder presenting the identification;
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or account holder presenting the identification;
4. An application appears to have been altered or forged, or gives the appearance of having been destroyed and re-assembled.

C. The presentation of suspicious personal identifying information, including:
1. Personal identifying information provided is inconsistent when compared against external information sources used by FAU;
2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by FAU;
3. The social security number provided is the same as that submitted by another account holder;
4. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other account holders or other persons opening accounts;
5. The account holder or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
6. Personal identifying information provided is not consistent with personal identifying information that is on file with FAU;
7. When using security questions, the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. The unusual use of, or other suspicious activity related to, a covered account, such as:
1. Shortly following the notice of a change of address for a covered account, FAU receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account**;**
2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns;
3. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
4. A covered account that has been inactive for a reasonably lengthy period of time is used;
5. Mail sent to the account holder is returned repeatedly as undeliverable although transactions continue to be conducted in conns a manner ca0601 T9Ber caaaac --0c9014 Tw 2T**J** Tda manner1 1 Tf0 Tc 0

5. Reopen a covered account with a new account number;
6. Not open a new covered account;
7. Close an existing covered account, and/or
8. Determine no response is warranted under the particular circumstances.

B. In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect account holder identifying information:

1. Ensure that its websites are secure or provide clear notice that a website is not secure;
2. Ensure complete and secure destruction of paper documents and computer files containing account holder account information when a decision has been made to no longer maintain such information;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of social security numbers;
5. Ensure computer virus protection is up to date; and
6. Require and keep only the kinds of account holder information that are necessary for University purposes.

VIII. Periodic Updates to the Program

A. At periodic intervals established in the Program, or as required, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment.
B. Periodic reviews will include an assessment of which accounts are covered by the Program.
C. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.
D. Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to FAU and its account holders.

IX. Program Updates

The Office of Financial Affairs will periodically review and update this Program to reflect changes in risks to account holders and the soundness of the University from Identity Theft. In doing so, the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities shall be considered. After considering these factors, the Office of Financial Affairs will determine whether changes to the Program, including the listing of Red Flags and additional training, are warranted. If warranted, the Program shall be updated appropriately.

X. Duties Regarding Address Discrepancies

A. FAU may reasonably confirm that an address is accurate by any of the following means:

1. Verification of the address with the account holder;
2. Review of FAU’s records;
3.

4.

C. Any specific requirements should be specifically addressed in appropriate contract arrangements.

D. Contractors and service providers must notify FAU of any security incidents experienced, even if such incidents may not have led to any actual compromise of FAU's data.

XIV. Disposal of Personal Identifying Information

A. When documents contain personal identifying information are discarded, they should be placed inside a locked shred bin or immediately shredded.

B. When disposing of old computers and portable storage devices containing personal identifying information, a disc wiping utility program should be used.

C. Any CD-rom, DVD-rom, floppy disk, or flash drive containing personal identifying information should be disposed of by shredding, punching holes in, or incineration.

INITIATING AUTHORITY: Senior Vice President, Finance & Administration

---

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: __5.6__