Butler University
Policy & Procedure

Policy: Identity Theft Information – Storage, Disposal, Breach & Red Flags **Policy Number:**
Dept. Responsible: Information Resources & Finance
Effective Date: June 1, 2009 **Rev. Date:**

1.0 OVERVIEW/PURPOSE

Butler University desires to protect the privacy of its constituents and to prevent the theft of confidential information we maintain. In order to minimize the risk of identity theft and to comply with applicable federal and state laws, this document outlines procedures pertaining to information that is in Butler's possession and confirms our obligation to notify affected parties in the event of a breach or suspicious activity.

The Federal Trade Commission (FTC) requires that many types of companies implement an Identity Theft Prevention Program (ITPP). Section 114 of the Fair and Accurate Transactions Act (FACT Act) mandated that the FTC regulate identity theft issues. As a result, the FTC has set forth the ITPP requirement in 16 C.F.R. & 681.2. Identity theft is defined as a fraud committed or attempted using identifying information of another person without authority.

Butler University has adopted the program set forth in this document to comply with FTC rules and regulations. In addition to being required by Federal Law, Butler University believes that it is a good practice to implement such a program in order to protect sensitive information from being used for improper purposes.

2.0 SCOPE

This policy applies to faculty, staff and all others performing tasks on behalf of Butler University, including but not limited to contractors, affiliates, guest instructors, student workers, and third-party providers, as it is through the diligent efforts of everyone that information is protected.

3.0 POLICY

3.1 Identity theft information – defined as data considered confidential by state and federal law that can assist or lead to identity theft. For this policy these fields include:

- Social Security number
- Driver's license number
- State ID card number
- Credit or debit card number, expiration date, security verification code
- Financial account number
- Butler University issued passwords

owned desktop computers, laptops, personal home computers, portable storage devices such as USB thumb drives or hard drives, CDs or DVDs, laptops regardless of who owns the device, PDAs and cell phones. Each individual is responsible to ensure identity theft information is stored in compliance with this policy.

E. Usernames and passwords which allow access to the Butler network or applications must not be stored, without special encryption, on a mobile device.

F. Identity theft information shall not

B.

6) Changing any passwords, security codes, or other security devices that permit access to accounts involved in the incident; or
7) Determining that no response is warranted under the particular circumstances. ;

3) A material change in the use of credit, especially with respect to recently established credit relationships; or
4) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

4.4 Suspicious Documents

Red flags may also include the following:

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

B. The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification.

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

E. Other information on the identification is not consistent with readily accessible information that is on file with Butler.

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

4.5 Suspicious Personal Identifying Information

The following items may be red flags:

A. Personal identifying information provided is inconsistent when compared against external information sources used by Butler. For example:
   1) The address does not match any address in the consumer report;
   2) The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
   3) Personal identifying information provided by the employee or student is not consistent with other personal identifying information provided by the person. For example, there might be a lack of correlation between the SSN range and date of birth.

B. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by Butler. For example, an address provided on one document is the same as the address provided on a different, but fraudulent, document.

C. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Butler. For example:
   1) The address on a document is fictitious or a mail drop;
   2) The phone number is invalid or is associated with a pager or answering service; or
   3) The request was made from a non-Butler issued e-mail account.

D. The SSN provided is the same as that submitted by other employees, students or other affected parties.

E. 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 employees, students or other affected parties.

F. The person opening the covered account fails to provide all required personal identifying information.

G. Personal identifying information provided is not consistent with personal identifying information that is on file with Butler.

H. When using security questions (mother's maiden name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

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

Red flags may further include the following:

A. Mail sent to the employee, student or other affected party is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.

B. We are notified that the employee or student is not receiving paper account statements.

C. We are notified of unauthorized activity in connection with an employee's or student's covered account.

D. We receive notice from employees, students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by Butler. .

E. We are notified by an employee, student, a victim of identity theft, a law enforcement authority, or any other person that Butler has opened a fraudulent account for a person engaged in identity theft.

5.0 Responding to Red Flags

Once potentially fraudulent activity is detected, all individuals must act quickly as a rapid appropriate response can protect Butler and any affected person from damages and loss.

A. Once potentially fraudulent activity is detected, the employee must gather all related documentation, write a description of the situation and present this information to the Vice President for Finance for determination.

B. The Vice President for Finance will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

C. If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1) Denying access to the covered account until other information is available to eliminate the red flag;
2) Canceling the transaction;
3) Notifying and cooperating with appropriate law enforcement;
4) Determining the extent of Butler liability;
5) Notifying the affected person that fraud has been attempted;
6) Changing any passwords, security codes, or other security devices that permit access to a covered account; or
7) Determining that no response is warranted under the particular circumstances.

6.0 Compliance

A. All devices are subject to a periodic audit to ens3 02 146.18 TmE3

B. All Butler faculty, staff, and affiliates must sign the Code of Responsibility Form, which will be maintained by Human Resources.

4(0)-1 292.13 711.61 0 0 1)a2JETBT1 0 0 1 172.46 7264.050 0 1 292.13 711.61 0 0 1)a22 g0 G -0.1437 Tc[B.)]TJET72.46 725