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

The Butler ID number (employee id field) and federal tax ID number (vendor id) do not require the special protection afforded the other fields listed above. However, reasonable care should be taken to protect all Butler confidential information; see section 8 for other related policies.

3.1 Policy Statement

Information classified as identity theft information should be collected, used, and retained only when there is a clear organizational requirement. Access to identity theft information should be provided only to those individuals involved in the Butler activity which requires access to or use of such information. Use of alternate data, such as a Butler ID number, the last four digits of a credit card (versus the whole number), or noting as "on file" should be used whenever possible. Identity theft information, whether in paper or electronic form, must be securely stored and disposed of in an approved and confidential manner.

3.2 Paper Records and Reports – Storage

A. Paper records and reports containing identity theft information as described above must be kept in locked drawers, cabinets or storage rooms or otherwise kept secure until appropriately discarded.

B. Desks, work areas, printers, and fax machines will be cleared of all documents containing identity theft information when the documents are not in use.

3.3 Paper Records and Reports – Disposal

A. Paper records and reports will be disposed of by placement in a Butler-designated, locked collection container or Butler-designated, approved high security shredder intended for identity theft information or other confidential information. Standard recycle bins or standard trash containers are not to be used to dispose of documents and reports that contain identity theft information.

B. The Butler confidential containers are emptied by an outside bonded firm; the material is shredded and then recycled. Questions on containers or pick-up schedule should be directed to the Director of Building Services.

C. Paper not containing any confidential information should go into Butler's standard recycle bins.

3.4 Electronic Media – Storage

A. Storage of identity theft information should be limited to only the data fields required to perform the university function.

B. Identity theft information should be stored only on either Butler-managed file servers (i.e., BUfiles) or within Butler central administrative systems (i.e., PeopleSoft, RecruitmentPlus, Advance).

C. Computers, laptops, smart phones and mobile storage devices are very popular because of their convenience; however, this is accompanied by risks since these devices are more easily compromised by hackers and/or may be accidentally misplaced. Typical end-user passwords on such devices, per law, do NOT provide sufficient protection for identity theft information.

D. **Identity theft information as defined in this policy should NOT reside on any individual-use computer or mobile device.** This includes, but is not limited to: Butler-

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 be stored on a non-Butler device, except when an official service agreement, in writing, is in place with an outside party (see 3.8).

3.5 Electronic Media – Disposal

When replacing or discarding any Butler device, it must be sent to Information Resources for proper disposal to ensure all data is permanently removed. Information Resources will clean the devices using data destruction software.

3.6 Exception for Computers or Mobile Devices

If university needs warrant storage of identity theft information on mobile devices, it must be approved in writing by the applicable vp, dean or executive director and the chief information officer (CIO). If approved, then the following guidelines must be observed:

A. Users of mobile devices containing identity theft information must take all reasonable and appropriate precautions to protect and control these devices from unauthorized access, tampering, loss, or theft, and should not leave the device unattended in public locations.

B. Identity theft information must be protected by at least a complex password. However, it is preferred that the data be stored in an approved encrypted format.

C. Any mobile device that is capable of using anti-virus software must have an installed and running antivirus program with up-to-date virus definitions.

D. Portable storage devices such as USB keys and hard drives must be placed in a locked storage facility when not in use.

E. Security updates relevant to the device must be applied promptly unless advised against installation by Information Resources.

F. Devices having access to identity theft information should have a password protected screen saver with an inactivity time-out.

G. Information stored must be limited to the minimum required to accomplish the function and be deleted as soon as it is no longer needed.

H. If a device is lost or stolen, the applicable dean or executive director and the chief information officer (CIO) must be notified immediately so that all appropriate disclosures may be made to the affected parties.

3.7 Information Transfer & Email

A. All transfers of identity theft information or other sensitive data to external entities should use an encrypted file transfer method approved by Information Resources; contact Information Resources for procedures.

B. Identity theft information may be sent between Butler constituents when the email is to another person **within Butler and the email is accessed via Butler's Outlook Exchange or BUmail** web interface (as those are secured).

C. Identity theft information should not be transferred via email to any party with a **non-Butler email account,** including organizations that have an official relationship with Butler. Traditional email via the public internet is not a secure or safe way to transfer fields such as social security numbers & credit card numbers.

D. Individuals who regularly handle identity theft information via email inside Butler should not forward their Butler email to a non-Butler account, such as a home or personal account.

E. Any paper reports sent externally, which contain identity theft information, should contain the following statement:

"This contains Butler University confidential information and is intended for the person/entity to which it was addressed. Any use by others is strictly prohibited."

3.8 Service Providers

A. Butler will ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

B. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

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

3.9 Breach

Any breach or exposure of identity theft information, either paper or electronic, must be reported and appropriate steps taken.

A. A breach of security includes:

1) Improper disposal of any media (paper or electronic) containing identity theft information
2) Unauthorized acquisition or transfer of data (paper or electronic) that compromises the security, confidentiality, or integrity of identity theft information.
3) Loss of electronic devices that includes identity theft information.

B. In the event of a breach, the party must immediately notify their supervisor who will notify their vice president, executive director or dean and the chief information officer (CIO).

C. In the event of a breach, Butler will then initiate the appropriate course of action per Butler policy and applicable laws. Actions may include:

1) Determining extent of breach and extent that information has potentially been compromised;
2) Notifying appropriate individuals affected by the exposure of their identity theft information;
3) Notifying and cooperating with appropriate law enforcement;
4) Notifying credit reporting agencies;
5) Determining the extent of Butler's liability;

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.

D. Indiana Code (IC 24-4-14) indicates breach has occurred per law whenever:

1) Social Security number is disclosed when not encrypted and includes more than five digits

-or-

2) Individual's first and last name or first initial and last name and one or more of the following are disclosed:

i. Driver's license number
ii. State ID card number
iii. Credit card number, or
iv. Financial account number/debit card number and security code/password, or access code.

4.0 "Red Flagging" of possible ID fraud

4.1 Covered Accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing employee or student account that meets the following criteria is also covered by this policy:

A. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or

B. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of Butler from identity theft, including financial, operational, compliance, reputation, or litigation risks.

4.2 Red Flags

Red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification. 4.3 A through 4.3 E identify various red flags applicable to Butler's covered accounts.

4.3 Red Flags – Notifications or Warnings From a Consumer Reporting Agency

A. Alerts, notifications or warnings from a consumer reporting agency;

B. A fraud or active duty alert included with a consumer report;

C. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

D. A notice of address discrepancy from a consumer reporting agency.

E. To the extent that consumer/credit reports are obtained and reviewed at any time, Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an individual, such as**:**

1) A recent and significant increase in the volume of inquiries;
2) An unusual number of recently established credit relationships;

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 ensure compliance.

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

C. Violators of this policy may be subject to disciplinary action up to and including dismissal.

7.0 Administration

A. Operational responsibility of this policy is delegated to the Vice President for Finance and Chief Information Officer. Periodically or as required, this policy will be reviewed by the CFO and CIO to ensure the policy is up-to-date and applicable in the current environment. Factors which may lead to re-evaluation or review include: the experiences of Butler with identity theft or changes in methods of identity theft, changes in the types of services Butler provides, and changes to or additional federal or state laws. All policy revisions will be reviewed and approved by the Board of Trustees.

B. Periodic reports will be made to the Board of Trustees in the event of material breaches or responses to red flags.

C. Annual staff training will be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with red flag covered accounts that may constitute a risk to Butler or its employees, students or other affected parties.

8.0 Related Policies

A. Computer Use Policy

B. Employee Code of Responsibility for Security and Confidentiality of Information

C. FERPA (Family Educational Rights and Privacy Act) -- see Student Handbook

D. HIPAA (Health Insurance Portability and Accountability Act)

9.0 Revision History

- Created April 2009 and effective June 1, 2009