



Cumberland UNIVERSITY

IDENTITY THEFT PREVENTION POLICY FRAMEWORK AND GUIDELINES

1. PURPOSE

The protection of Confidential and Sensitive Information assets and the resources that support them are critical to the operation of Cumberland University (known from this point as “the University”). As information assets are handled they are placed at risk for potential threats of employee errors, malicious or criminal actions, theft, and fraud. Such events could cause the University to incur a loss of confidentiality or privacy, financial damages, fines, and penalties.

The purpose of this policy is to reduce the risk of a loss or breach of Confidential and Sensitive Information through guidelines designed to detect, prevent, and mitigate loss due to errors or malicious behavior. The University recognizes that absolute security against all threats is an unrealistic expectation. Therefore, the goals of risk reduction and implementation of this policy are based on:

- An assessment of the Confidential and Sensitive Information handled by the University.
- The cost of preventative measures designed to detect and prevent errors or malicious behavior.
- The amount of risk that the University is willing to absorb.

These policy guidelines were derived through a risk assessment of the University methods of handling Confidential and Sensitive Information. Determination of appropriate security measures must be a part of all operations and shall undergo periodic evaluation.

2. SCOPE

These policies apply to all employees of and service providers of the University. This includes all parties that may come into contact with Confidential and Sensitive Information, such as, contractors, consultants, temporaries, and personnel of third party affiliates.

The University will implement and enforce these policies, as well as, design more specific or new guidelines as needed.

3. EFFECTIVE DATE

This Identity Theft Prevention Policy is considered to be in force as of December 31, 2010.

4. DEFINITIONS

4.1. Confidential and Sensitive Information (CSI)

Confidential and Sensitive Information includes, but is not limited to, the following identifiers whether contained in hard copy or electronic format:

4.1.1. Personal Information

- 4.1.1.1. Social Security Number
- 4.1.1.2. Social Insurance Number
- 4.1.1.3. Date of Birth
- 4.1.1.4. Mother's Maiden Name
- 4.1.1.5. Driver's License Information
- 4.1.1.6. Professional License Information
- 4.1.1.7. Paychecks, Pay stubs, Pay rates
- 4.1.1.8. Passport Information

4.1.2. Financial Information

- 4.1.2.1. Credit Card Numbers
- 4.1.2.2. Credit Card Expiration Dates
- 4.1.2.3. Credit Card CCV Numbers
- 4.1.2.4. Bank/Credit Union Account Numbers
- 4.1.2.5. Billing Information
- 4.1.2.6. Payment History

4.1.3. Medical Information

- 4.1.3.1. Medical Records
- 4.1.3.2. Doctor Names and Claims
- 4.1.3.3. Health, Life, Disability Insurance Policy Information
- 4.1.3.4. Prescription Information

4.1.4. Business Information

- 4.1.4.1. Federal ID Numbers
- 4.1.4.2. Proprietary Information
- 4.1.4.3. Trade Secrets
- 4.1.4.4. Business Systems
- 4.1.4.5. Security Systems
- 4.1.4.6. Employee Identifiers
- 4.1.4.7. Student Identifiers
- 4.1.4.8. Access Numbers / Passwords
- 4.1.4.9. Customer, Student, Patient Identifiers
- 4.1.4.10. Vendor Numbers
- 4.1.4.11. Account Numbers

4.2. Account

An account is a body of information, or a record, or an individual, group, or entity that is kept for the purpose of transacting on an on-going basis with another individual, group, or entity. The terms "accounts" and "records" are used interchangeably because they share similar functions and

characteristics. Both contain identifiable information on an individual, group, or entity. They each allow for access to products or services, and keep a history of transaction activity.

4.3. Covered Account

Both new and existing accounts where a continuing relationship exists between the University and an individual, group, or entity are considered “covered accounts.” There are two definitions.

4.3.1. An account that the University offers or maintains, primarily for personal, family, or household purposes, that involve or is designated to permit multiple payments or transactions. Examples include a credit card account, tuition and fee payment, bookstore purchases, and/or other financial transactions of matriculated and non-matriculated students and of employees.

4.3.2. Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or mitigation risks.

4.4. Electronic or Soft Copy Format

Electronic or Soft Copy Format refers to any Confidential and Sensitive Information that exists electronically on CDs, DVDs, phones, computers, networks, portable devices, etc.

4.5. Hard Copy Format

Hard Copy Format refers to any Confidential and Sensitive Information that exists physically on paper.

4.6. Physical Access Zone

A physical access zone is a clearly defined physical or implied boundary established to control and limit access to CSI areas.

4.7. Red Flags

Red Flags are patterns, practices, or specific activities involving covered accounts that indicate the possible risk of identity theft

4.8. Service Provider

A service provider is any individual, group, or entity that directly provides a service to the University or on behalf of the University for its customers or clients.

4.9. Spoken Word

Spoken Word refers to the transfer of Confidential and Sensitive Information verbally or audibly through electronic media.

5. ROLES AND RESPONSIBILITIES

5.1. University Administration

The University Administration is responsible for the design, implementation, and oversight of the Identity Theft Prevention Program. However, if it is not feasible for the University Administration to be directly involved, it may appoint a member of senior management to be charged with these responsibilities. This designated Identity Theft Prevention Officer must seek University Administration approval on policy decisions. They must report to the board at least annually on the state of the Identity Theft Prevention Program.

5.2. Identity Theft Prevention Officer

The Identity Theft Prevention Officer is responsible for the following:

- 5.2.1. Risk Assessment – Conduct periodic risk assessments of Confidential and Sensitive Information handling methods.
- 5.2.2. Design – Design of more specific or new policy guidelines as needed.
- 5.2.3. Implementation – Conduct training for employees on a periodic basis.
- 5.2.4. Monitor – Evaluate the policy and procedures regularly.
- 5.2.5. Enforce - Take disciplinary action with employees as needed.
- 5.2.6. Response Plan – Create a plan to respond to security incidents.

5.3. Employees

All personnel are responsible for adhering to these guidelines, and for reporting any security incidents to the Identity Theft Prevention Officer immediately.

5.4. Service Providers

The level of responsibility given to service providers for security reasons depends on the scope of their service offering. Each will be responsible according to their *direct* or *indirect* access to information. In either case, service providers will be held accountable for their conduct and agreements must delineate where the University's liability ends and where the service provider's liability begins.

- 5.4.1. **Direct Access to Information.** A service provider is considered to have direct access to information when they perform an activity with employee or customer information on behalf of the University. If information is shared, then the service provider must have an Identity Theft Prevention Policy that complies with or exceeds the best practices of colleges and universities.
- 5.4.2. **Indirect Access to Information.** A service provider is treated differently when they have indirect access to information. These are service providers that are working in the proximity of Confidential and Sensitive Information in the business, but their function does not

involve sharing information. In this type of relationship, the service provider must comply with this Identity Theft Prevention Policy.

6. POLICY GUIDELINES

The following policy guidelines cover issues related to the collection, retention, transfer, and destruction of Confidential and Sensitive Information.

6.1. Physical Access Zones

6.1.1. The University will establish, maintain, and enforce physical access zones in all of its facilities to control and limit access to CSI areas. There are four types of color coded zones, each with different access requirements.

6.1.1.1. Green Zones. Green zones are low priority public areas where everyone has access.

6.1.1.2. Yellow Zones. Yellow zones are moderate priority operational or information processing areas. All employees are authorized in these zones. Service providers, customers, and visitors must be accompanied by an employee.

6.1.1.3. Red Zones. Red zones are high priority areas containing proprietary information, record storage, or data bases. Access is limited to authorized employees only. All others must be identified, verified, and have an escort at all times.

6.1.1.4. Grey Zones. Grey zones are transition zones where risk fluctuates as CSI enters and leaves. The transition zone takes on the characteristics of other zone requirements when CSI is introduced. Conference rooms and vehicles are good examples.

6.2. Information Storage

Storing Confidential and Sensitive Information is a normal function of conducting business at the University. Employees shall only store CSI for legitimate business needs and those needs related to their individual job responsibilities.

6.2.1. Hard Copy Storage

6.2.1.1. On-site Storage

On-site storage refers directly to CSI stored within any University facility.

6.2.1.1.1. Employees Personal Belongings

The University will provide all personnel with a secure place to store personal belongings. Employees are responsible for keeping personal items secure during work hours.

6.2.1.1.2. CSI Stored in a Workspace

Confidential and Sensitive Information stored in an office, cubicle, reception area, cash register, or other workspace must be kept in locked desks, cabinets, closets, or lockers when not in use.

6.2.1.1.3. File Rooms and Storage Rooms

File and storage room doors must be closed and locked when unattended by authorized personnel.

6.2.1.1.4. Records Storage

Company, customer, transaction, and service provider records will only be stored when there is a legitimate business need. Any records in storage beyond the legal statute of limitations will be appropriately disposed of by designated employees.

6.2.1.2. Off-site Storage

Off-site storage refers to any place CSI is stored outside of designated University facilities.

6.2.1.2.1. Approved Storage Facilities

CSI may only be stored in facilities authorized by University Administration.

6.2.1.2.2. Storage Service Providers

All storage service providers must comply with the service provider oversight policies in this Identity Theft Prevention Policy.

6.2.2. Soft Copy Storage

Company representatives shall only store CSI on University authorized computers, telecommunications, or other electronic devices. A list of approved equipment will be maintained by the company's Identity Theft Prevention Officer or Information Technology Professional.

6.2.2.1. Encryption

All CSI stored on portable electronic devices or electronically transmitted must be encrypted.

6.2.2.2. Portable Electronic Devices

Portable electronic devices must be secured when not in use. The physical security of these devices is the responsibility of the authorized user. These include laptop computers, cell phones (specifically smart phones), jump drives, thumb drives, external hard drives, etc.

6.3. Destruction

6.3.1. Hard Copy Destruction

All hard copy CSI will be shred when it no longer has a legitimate business use.

6.3.1.1. In-house Storage awaiting shredding

6.3.1.1.1. is the responsibility of every department.

6.3.1.1.2. Hard copy material waiting to be shred will be maintained in locked and secured boxes labeled "Confidential Shred Material."

6.3.1.2. Destruction Service Providers

All destruction service providers must comply with the service provider oversight policies in this Identity Theft Prevention Policy.

6.3.1.2.1. All destruction service providers must be National Association of Information Destruction, Inc. (NAID, Inc) Certified.

6.3.1.2.2. The University must be provided a certificate of destruction every time material is released to be destroyed.

6.3.2. Soft Copy Destruction

All computers, telecommunications, or electronic devices must be “sanitized” or “wiped” clean before being sold, donated, or discarded. A member of senior management or an Information Technology professional is designated for this function.

6.4. Transferability

6.4.1. Spoken Word

6.4.1.1. Company representatives must identify and verify callers as authorized before releasing any CSI over the phone.

6.4.1.2. Company representatives may not release any CSI to a third party unless the third party was previously authorized in writing.

6.4.1.3. Employees may only discuss CSI with University-authorized individuals for a legitimate business purpose.

6.4.1.4. Under no circumstances are company representatives permitted to leave CSI messages on voicemail systems.

6.4.2. Hard Copy Transferability

6.4.2.1. Clean Desk Policy

Company representatives shall keep desks and workspaces clear of CSI when not in use.

6.4.2.2. Dry Erase, Chalk, and Bulletin Boards

Employees must not print, post, or make known any CSI on any dry erase boards, chalk boards, or bulletin boards in public or operations areas. Dry erase and chalk boards must be wiped clean after every use.

6.4.2.3. Transporting Information

6.4.2.3.1. Confidential and Sensitive information shall be transported from one external location to another in the locked trunk of a vehicle.

6.4.2.3.2. An inventory must be kept of all CSI hard copy that is shipped.

6.4.2.4. Facsimiles (FAX)

6.4.2.4.1. FAX machines must not be physically located in a public area. Electronic FAX delivery will occur using the

safest and most encrypted platform reasonably available in the marketplace.

6.4.2.4.2. Every outgoing fax must contain a coversheet containing the senders and receivers names. Each coversheet will contain the University's Confidential and Sensitive Information Disclaimer.

6.4.2.4.3. Employees sending a FAX containing CSI shall notify the recipient that the FAX is being sent.

6.4.2.4.4. Any unnecessary CSI must be masked or deleted before faxing.

6.4.3. Soft Copy Transferability

6.4.3.1. Personal Electronic Devices

Company representatives and service providers are only permitted to bring personal electronic devices into University facilities that are approved by University Administration.

6.4.3.2. E-mail Transferability

6.4.3.2.1. All outgoing email containing CSI must be encrypted.

6.4.3.2.2. Employees shall not respond to emails requesting CSI unless they first contact the sender and verify that the sender is authorized to have the information being requested.

6.4.3.3. Portable Electronic Device Transferability

Portable electronic devices must be secured when transported from one location to another. The physical security of these devices is the responsibility of the authorized user.

6.5. Information Accessibility

6.5.1. Hard Copy Accessibility

6.5.1.1. Entrances and Exits

All facility entrances and exits that are determined not for public use will remain locked at all times, unless it violates fire code.

6.5.1.2. Mail Accessibility

Mail must be kept in a secure area until requested by the postal carrier or received internally by the intended recipient who shows at least one photo identification to the mail handler.

6.5.1.3. Surveillance Equipment

The University reserves the right to use cameras and other surveillance equipment to monitor public, operations, and restricted areas.

6.5.1.4. Employee Authorization

6.5.1.4.1. Every employee will be thoroughly trained before

being authorized to handle CSI.

6.5.1.4.2. Employees shall only handle CSI for a legitimate business purpose and that is a function of their job responsibilities.

6.5.1.4.3. A written procedure and checklist will be used by management to terminate access when an employee is terminated from service.

6.5.1.5. Service Provider Accessibility

Service providers shall only handle CSI for a legitimate business purpose and that is a function of their job responsibilities as stated in their service provider agreements.

6.5.2. Soft Copy Accessibility

6.5.2.1. Technology System Audits

The University will conduct periodic technology system audits to test the integrity of technology information systems no less than annually.

6.5.2.2. Logging on and off Computers

6.5.2.2.1. Only authorized personnel may log onto University networks and equipment.

6.5.2.2.2. All personnel are required to log off computers when not in use.

6.5.2.3. Passwords

Employees shall use strong passwords containing a combination of numbers, letters, and characters. Passwords should be changed no less than once every (90) ninety days.

6.5.2.4. Personal Use of Technology Equipment

6.5.2.4.1. Employees are permitted to browse the internet with company equipment only for company purposes.

6.5.2.4.2. Employees are permitted to instant message using company equipment only for company purposes.

6.5.2.4.3. Employees are permitted to check personal email on company equipment.

6.5.2.5. Remote Access

Remote access to University networks must be approved using IT protocols and said access must be done with authorized resources.

6.6. Plan for a Loss or Breach

6.6.1. Information Security Audits

The Identity Theft Prevention Officer is authorized to conduct security audits of any area containing CSI at anytime to ensure the safety and security of that information.

6.6.2. Discovery of a Breach in the Workplace

6.6.2.1. Employee Protocol

6.6.2.1.1. Do not disturb the area.

6.6.2.1.2. Secure the area.

6.6.2.1.3. Notify manager or supervisor.

6.6.2.1.3.1. Manager will contact Identity Theft Prevention Officer

6.6.2.1.4. Document the event.

6.6.2.1.4.1. Submit to Identity Theft Prevention Officer.

6.6.2.2. Manager or Supervisor Protocol

6.6.2.2.1. Ensure affected area is secure. Do not let anyone use the phone or computer in that area.

6.6.2.2.2. Gather visitor logs, employee time sheets, list everyone who had access before, during, and after the incident.

6.6.2.2.3. Interview employee witness(es).

6.6.2.2.4. Contact ISO.

6.6.2.3. Identity Theft Prevention Officer Protocol

6.6.2.3.1. Determine that there is a breach

6.6.2.3.1.1. Interview Employee Witness

6.6.2.3.1.2. Review Security Incident Report

6.6.2.3.2. Contact the University attorney

6.6.2.3.3. Make a police report

6.6.2.3.4. Notify potential victims according to legal statutes.

6.6.2.3.5. Public relations and continuity considerations.

6.6.3. Discovery of a Breach through Accusation

6.6.3.1. Employee Protocol

6.6.3.1.1. Be sympathetic to the potential victim

6.6.3.1.2. Do not confirm or deny their allegations

6.6.3.1.3. Document the conversation

6.6.3.1.4. Document contact information

6.6.3.1.5. Inform them that your Identity Theft Prevention Officer will contact them.

6.6.3.2. Identity Theft Prevention Officer Protocol

6.6.3.2.1. Interview Employee Witness

6.6.3.2.2. Review Security Incident Report

6.6.3.2.3. Contact potential victim.

6.6.3.2.4. Ask them to reiterate their story.

- 6.6.3.2.5. Assure them that you will look into it.
- 6.6.3.2.6. Contact your attorney.
- 6.6.3.2.7. Determine that there is a breach
- 6.6.3.2.8. Assess the extent of damage
- 6.6.3.2.9. Make a police report
- 6.6.3.2.10. Notify potential victims according to legal statutes.
- 6.6.3.2.11. Public relations and continuity considerations

6.7. Suspicious Behavior

- 6.7.1. University representatives shall document and confidentially report to senior management any suspicious behavior on behalf of other employees, customers, service providers, or visitors.
- 6.7.2. Employees should challenge, verify, and escort any visitor or service provider found in or requesting access to a non-public area. Employees should get assistance and are not expected to engage in a situation if they are in fear of their physical safety.

6.8. Transaction Identification and Verification

The University requires company representatives to verify adequate means of identification from a person before they can transact business with a check, credit card, or debit card on behalf of themselves, a group or an entity.

6.8.1. Personal or Company Check Transactions

University representatives must not accept a check for payments without adequately verifying at least one form of identification from the following list of current and non-expired forms of identification.

- 6.8.1.1. US State Driver's License
- 6.8.1.2. US State Picture ID
- 6.8.1.3. US Passport
- 6.8.1.4. US Military ID
- 6.8.1.5. US Federal ID
- 6.8.1.6. Alien Registration Card
- 6.8.1.7. Physical Address
- 6.8.1.8. Phone Number
- 6.8.1.9. Valid Signature
- 6.8.1.10. Other

6.8.2. Credit or Debit Card Transactions

University representatives must not accept credit card or debit card payments without adequately verifying at least one form of identification from the following list of current and non-expired forms of identification.

- 6.8.2.1. US State Driver's License

- 6.8.2.2. US State Picture ID
- 6.8.2.3. US Passport
- 6.8.2.4. US Military ID
- 6.8.2.5. US Federal ID
- 6.8.2.6. Alien Registration Card
- 6.8.2.7. Physical Address
- 6.8.2.8. Credit / Debit Card Number
- 6.8.2.9. Expiration Date
- 6.8.2.10. CVC2 / CVV2 / CID
- 6.8.2.11. Valid Signature
- 6.8.2.12. Other

6.9. New and Existing Account Identification and Verification

University representatives shall make a reasonable effort to identify and verify each customer's identity when opening new accounts or accessing existing accounts.

6.9.1. New Accounts

Opening new accounts requires one of the following identification, document and non-document verification.

6.9.1.1. Customer Identifying Information

- 6.9.1.1.1. Legal Name
- 6.9.1.1.2. Date of Birth
- 6.9.1.1.3. Physical Address
- 6.9.1.1.4. Social Security Number
- 6.9.1.1.5. EIN
- 6.9.1.1.6. Passport and Country of Issuance
- 6.9.1.1.7. Alien Identification Card Number
- 6.9.1.1.8. Power of Attorney
- 6.9.1.1.9. Other

6.9.1.2. Verification with Documents

When opening new accounts company representatives must request two sources of identification, one primary and one secondary.

- 6.9.1.2.1. Primary Identification
 - 6.9.1.2.1.1. US State Picture Driver's License
 - 6.9.1.2.1.2. US State Picture Issued ID Card
 - 6.9.1.2.1.3. US Passport
 - 6.9.1.2.1.4. US Military Picture ID

- 6.9.1.2.1.5. Federal Picture ID
- 6.9.1.2.1.6. Alien Registration Card
- 6.9.1.2.1.7. Other

6.9.1.2.2. Secondary Identification

- 6.9.1.2.2.1. Social Security card
- 6.9.1.2.2.2. Individual taxpayer identification card
- 6.9.1.2.2.3. EIN
- 6.9.1.2.2.4. Voter registration, state of residence
- 6.9.1.2.2.5. Birth Certificate
- 6.9.1.2.2.6. Credit card
- 6.9.1.2.2.7. Bank cards
- 6.9.1.2.2.8. Insurance Cards
- 6.9.1.2.2.9. State government
- 6.9.1.2.2.10. Local government
- 6.9.1.2.2.11. Company identification
- 6.9.1.2.2.12. Police identification
- 6.9.1.2.2.13. Temporary driver license
- 6.9.1.2.2.14. US Federal Government issued Permanent Resident Card
- 6.9.1.2.2.15. US Federal Government issued Employment Authorization
- 6.9.1.2.2.16. Other

6.9.1.3. Alternative Documents for Elderly or Disabled

- 6.9.1.3.1. Utility Bill: telephone, electricity, gas, water.
- 6.9.1.3.2. Voters Registration
- 6.9.1.3.3. State issued birth certificate
- 6.9.1.3.4. Company retirement check payable to individual.
- 6.9.1.3.5. Federal or state or county benefit check issued to individual.
- 6.9.1.3.6. Court documents indicating custodian or fiduciary appointment
- 6.9.1.3.7. Social Security Card.
- 6.9.1.3.8. Individual Tax Identification Card
- 6.9.1.3.9. Other

6.9.1.4. Non-Document Verification

Company representatives must follow-up document verification with non-document verification. Acceptable forms of non-document verification are:

- 6.9.1.4.1. Credit report
- 6.9.1.4.2. Previous bank/credit union reference
- 6.9.1.4.3. Site visit
- 6.9.1.4.4. Telephone call to customer
- 6.9.1.4.5. Letter of Welcome
- 6.9.1.4.6. Public data base
- 6.9.1.4.7. Financial Statement
- 6.9.1.4.8. Professional papers
- 6.9.1.4.9. certified articles of incorporation
- 6.9.1.4.10. Partnership agreement
- 6.9.1.4.11. Association resolution
- 6.9.1.4.12. Assumed name certificate
- 6.9.1.4.13. Trust agreement
- 6.9.1.4.14. Business license
- 6.9.1.4.15. Criminal Background Check
- 6.9.1.4.16. Medical Information Bureau (MIB) File
- 6.9.1.4.17. Other

6.9.2. Existing Accounts

Customer access of existing accounts requires the following identification, document and non-document verification depending upon the mode of operation.

6.9.2.1. Account Access in Person

6.9.2.1.1. Verification with Documents

When a customer wishes to access existing accounts, company representatives must request two sources of identification, one primary and one secondary

6.9.2.1.1.1. Primary Identification

- 6.9.2.1.1.1.1. US State Picture Driver's License
- 6.9.2.1.1.1.2. US State Picture Issued ID Card
- 6.9.2.1.1.1.3. US Passport
- 6.9.2.1.1.1.4. US Military Picture ID

- 6.9.2.1.1.1.5. Federal Picture ID
- 6.9.2.1.1.1.6. Alien Registration Card
- 6.9.2.1.1.1.7. Other

6.9.2.1.1.2. Secondary Identification

- 6.9.2.1.1.2.1. Social Security card
- 6.9.2.1.1.2.2. Individual taxpayer identification card
- 6.9.2.1.1.2.3. EIN
- 6.9.2.1.1.2.4. Voter registration, state of residence
- 6.9.2.1.1.2.5. Birth Certificate
- 6.9.2.1.1.2.6. Credit card
- 6.9.2.1.1.2.7. Bank cards
- 6.9.2.1.1.2.8. Insurance Cards
- 6.9.2.1.1.2.9. State government
- 6.9.2.1.1.2.10. Local government
- 6.9.2.1.1.2.11. Company identification
- 6.9.2.1.1.2.12. Police identification
- 6.9.2.1.1.2.13. Temporary driver license
- 6.9.2.1.1.2.14. US Federal Government issued Permanent Resident Card
- 6.9.2.1.1.2.15. US Federal Government issued Employment Authorization
- 6.9.2.1.1.2.16. Other

6.9.2.1.1.3. Alternative Documents for Elderly or Disabled

- 6.9.2.1.1.3.1. Utility Bill: telephone, electricity, gas, water.
- 6.9.2.1.1.3.2. Voters Registration
- 6.9.2.1.1.3.3. Family Bible, on the “Birth” page the individual’s name and date of birth
- 6.9.2.1.1.3.4. State issued birth certificate
- 6.9.2.1.1.3.5. Company retirement check payable to individual.
- 6.9.2.1.1.3.6. Federal or state or county benefit check issued to individual.
- 6.9.2.1.1.3.7. Court documents indicating

custodian or fiduciary appointment

6.9.2.1.1.3.8. Social Security Card.

6.9.2.1.1.3.9. Individual Tax Identification Card

6.9.2.1.1.3.10. Other

6.9.2.2. Account Access On-Line

6.9.2.2.1. Customer Identifying Information

6.9.2.2.1.1. Legal Name

6.9.2.2.1.2. Date of Birth

6.9.2.2.1.3. Physical Address

6.9.2.2.1.4. Account Number

6.9.2.2.1.5. Policy Number

6.9.2.2.1.6. Student Number

6.9.2.2.1.7. Social Security Number

6.9.2.2.1.8. EIN

6.9.2.2.1.9. Personal Identification Number

6.9.2.2.1.10. User ID

6.9.2.2.1.11. Password

6.9.2.2.1.12. Email Address

6.9.2.2.1.13. Personal Knowledge Questions

6.9.2.2.1.14. Other

6.9.2.3. Account Access By Phone

6.9.2.3.1. Customer Identifying Information

6.9.2.3.1.1. Legal Name

6.9.2.3.1.2. Date of Birth

6.9.2.3.1.3. Physical Address

6.9.2.3.1.4. Account Number

6.9.2.3.1.5. Policy Number

6.9.2.3.1.6. Student Number

6.9.2.3.1.7. Social Security Number

6.9.2.3.1.8. EIN

6.9.2.3.1.9. Personal Identification Number

6.9.2.3.1.10. User ID

6.9.2.3.1.11. Password

6.9.2.3.1.12. Email Address

6.9.2.3.1.13. Personal Knowledge Questions

6.9.2.3.1.14. Other

6.9.2.4. Account Access By Mail

6.9.2.4.1. Customer Identifying Information

6.9.2.4.1.1. Legal Name

6.9.2.4.1.2. Date of Birth

6.9.2.4.1.3. Physical Address

6.9.2.4.1.4. Account Number

6.9.2.4.1.5. Policy Number

6.9.2.4.1.6. Student Number

6.9.2.4.1.7. Social Security Number

6.9.2.4.1.8. EIN

6.9.2.4.1.9. Personal Identification Number

6.9.2.4.1.10. User ID

6.9.2.4.1.11. Password

6.9.2.4.1.12. Email Address

6.9.2.4.1.13. Personal Knowledge Questions

6.9.2.4.1.14. Letter of Instruction

6.9.2.4.1.15. Signature Guarantee

6.9.2.4.1.16. Notarization

6.9.2.4.1.17. Power of Attorney

6.9.2.4.1.18. Other

6.10. Red Flags

6.10.1. Alerts, Notifications or Warnings from a Consumer Reporting Agency

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

6.10.1.2. A customer reporting agency provides a notice of credit freeze in response to a consumer report.

6.10.1.3. A consumer reporting agency provides a notice of address discrepancy.

6.10.1.4. 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 inquires; b) an unusual number of recently established credit relationship; 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.

6.10.1.5. Other

6.10.2. Suspicious Documents

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

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

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

6.10.2.4. 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.

6.10.2.5. An application appears to be altered or forged, or gives the appearance of being reassembled.

6.10.2.6. Other

6.10.3. Suspicious Identifying Personal Information

6.10.3.1. Personal identifying information provided is inconsistent when compared to external information sources used by the financial institution or creditor. For example: a) The address does not match any address on the consumer; or b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

6.10.3.2. Personal identifying information provided by the consumer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and the date of birth.

6.10.3.3. Personal identifying information 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.

6.10.3.4. Personal identifying information 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 prison; or b) The phone number is invalid, or is associated with a pager or answering service.

6.10.3.5. The SSN provided is the same as that submitted by

other persons.

6.10.3.6. 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.

6.10.3.7. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

6.10.3.8. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

6.10.3.9. For 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.

6.10.3.10. Other

6.10.4. Unusual Use of, Suspicious Activity Related to, the Covered Account

6.10.4.1. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards, or a cell phone, or for additional authorized users on the account.

6.10.4.2. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: a) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g.- electronic equipment or jewelry); or b) the customer fails to make the first payment or makes an initial payment but no subsequent payments.

6.10.4.3. 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) non-payment 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.

6.10.4.4. 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).

6.10.4.5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in

connection with the customer's covered account.

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

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

6.10.5. Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

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

6.11. Red Flags Response

6.11.1. Response to Alerts, Notifications or Warnings from a Consumer Reporting Agency

When a company representative is presented with an alert, notification or warning from a consumer reporting agency, they must act quickly in an effort to prevent or mitigate loss for the customer and the University.

Appropriate responses are as follows:

- 6.11.1.1. Take additional steps to verify identity.
- 6.11.1.2. Flag relevant accounts.
- 6.11.1.3. Monitor account activity.
- 6.11.1.4. Decline account application.
- 6.11.1.5. Validate address.
- 6.11.1.6. Document with a Suspicious Activity Report (SAR).
- 6.11.1.7. Notify existing customer on record.
- 6.11.1.8. Other

6.11.2. Response to Suspicious Documents

In the course of business, a company representative may be presented with suspicious documents. Appropriate responses are as follows:

- 6.11.2.1. Verify using third party resources.
- 6.11.2.2. Verify using existing account records.
- 6.11.2.3. Decline application.
- 6.11.2.4. Decline account access.
- 6.11.2.5. Document with a Suspicious Activity Report (SAR).
- 6.11.2.6. Notify law enforcement (if necessary)
- 6.11.2.7. Notify existing customer on record

6.11.2.8. Other

6.11.3. Response to Suspicious Identifying Personal Information

When a person provides suspicious or inconsistent identifying information to a company representative, the response is as follows:

- 6.11.3.1. Escalate verification to a higher level.
- 6.11.3.2. Decline account application.
- 6.11.3.3. Decline account access.
- 6.11.3.4. Notify existing customer on record.
- 6.11.3.5. Change account access information.
- 6.11.3.6. Change account numbers.
- 6.11.3.7. Document with a Suspicious Activity Report (SAR).
- 6.11.3.8. Involve law enforcement.
- 6.11.3.9. Other

6.11.4. Response to Unusual Use of, Suspicious Activity Related to, the Covered Account

Company representatives shall be vigilant in protecting customer accounts when transacting, servicing, or processing business. When suspicious activity or unusual patterns emerge in covered accounts, the appropriate responses are as follows:

- 6.11.4.1. Use Personal Knowledge questions for verification.
- 6.11.4.2. Validate address.
- 6.11.4.3. Decline account access.
- 6.11.4.4. Document with a Suspicious Activity Report (SAR).
- 6.11.4.5. Notify existing customer on record.
- 6.11.4.6. Change account access information.
- 6.11.4.7. Change account numbers.
- 6.11.4.8. Involve law enforcement.
- 6.11.4.9. Other

6.11.5. Response to Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

Company representatives that are notified of a security incident from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts must immediately inform senior management and the Identity Theft Prevention Officer. Appropriate responses are as follows:

- 6.11.5.1. Decline account access.

- 6.11.5.2. Close fraudulent account.
- 6.11.5.3. Document with a Suspicious Activity Report (SAR).
- 6.11.5.4. Notify existing customer on record.
- 6.11.5.5. Open new account.
- 6.11.5.6. Do Not Attempt to Collect on the Fraudulent Account from the True Identity.
- 6.11.5.7. Cooperate with law enforcement..
- 6.11.5.8. Other

6.12. Staff Training

- 6.12.1. Staff training in relation to the Identity Theft Prevention Program and its policies shall be conducted for all employees, temps, independent representatives, and contractors, both part-time and full-time, on a periodic basis no less than once annually.
- 6.12.2. Staff members will receive additional training triggered by changes in policy, changes in their mode of operations, security incidents, and new information.

6.13. Service Provider Oversight

- 6.13.1. The University will periodically review all service provider agreements and activities no less than annually.
- 6.13.2. A service provider with direct access to CSI must provide proof of, and maintain, their own Identity Theft Prevention Program that is consistent with, or exceeds, the University's industry regulations.
- 6.13.3. A service provider that has indirect access to CSI shall comply with this Identity Theft Prevention Policy.

7. ENFORCEMENT

The Identity Theft Prevention Officer has the authority to enforce this policy. Any employee, temporary, contractor, or consultant found in violation may be subject to disciplinary action, up to and including termination of employment.