Red Flags Policy

Effective Date

Policy

Document Number: REDFLAG--101
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about the effective date of the Red Flags Identity Theft Prevention Policy.

Purpose: Delineation of information.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Policy Provisions

1. Effective Date

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

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Scope of Red Flags Identity Theft Policy

Info Sheet

Document Number: REDFLAG--101d
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

List:

1. Scope of Red Flags Identity Theft Policy

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.

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Regulations

federal mandate
Peer review standards
Standards of good practice
University governance

Definitions of Confidential and Sensitive Information (CSI)

Policy

Document Number: REDFLAG--102
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about confidential and sensitive information (CSI).

Purpose: Delineation of policy and definitions.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Fine

Loss of privilege, general

Termination
Staff members who knowingly and blatantly violate this policy may be terminated.

Policy Provisions

1. Definitions of 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.

   1.1 Personal Information

   1. Social Security Number
   2. Social Insurance Number
   3. Date of Birth
   4. Mother's Maiden Name
   5. Driver's License Information
   6. Professional License Information
   7. Paychecks, Pay stubs, Pay rates
   8. Passport Information

1.2 Financial Information

1. Credit Card Numbers
2. Credit Card Expiration Dates
3. Credit Card CCV Numbers
4. Bank/Credit Union Account Numbers
5. Billing Information
6. Payment History

1.3 Medical Information

1. Medical Records
2. Doctor Names and Claims
3. Health, Life, Disability Insurance Policy Information
4. Prescription Information

1.4 Business Information

1. Federal ID Numbers
2. Proprietary Information
3. Trade Secrets
4. Business Systems
5. Security Systems
6. Employee Identifiers
7. Student Identifiers
8. Access Numbers / Passwords
9. Customer, Student, Patient Identifiers
10. Vendor Numbers
11. Account Numbers

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.

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.

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.
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. 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.

5. Hard Copy Format

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

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.

7. Red Flags

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

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.

9. Spoken Word

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

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Roles and Responsibilities

Policy

Document Number: REDFLAG--103
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Definitions of roles and responsibilities relative to the Red Flags Identity Theft Policy.

Purpose: Delineation of definitions.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Policy Provisions

1. Roles and Responsibilities

1.1 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.

1.2 Identity Theft Prevention Officer

The Identity Theft Prevention Officer is responsible for the following:

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

1.3 Employees

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

1.4 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.

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.
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.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Enforcement

Info Sheet

Document Number: REDFLAG--103d
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

List:

1. 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.

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Regulations

federal mandate

Policy Guidelines

Policy

Document Number: REDFLAG--104
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about policy guidelines relative to the Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility:
Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Policy Provisions

1. Policy Guidelines (PG)

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

Performance Evaluation

Performance Metrics:
Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

PG--Physical Access Zones

Policy

Document Number: REDFLAG--105
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about physical access zones relative to the Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. Physical Access Zones

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.

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

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

VP of Business and Finance

PG--Information Storage

Policy

Document Number: REDFLAG--106
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about storage of information relative to the Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Policy Provisions

1. 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.

1.1 Hard Copy Storage

1.1.1 On-site storage

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

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.

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.

3. **File Rooms and Storage Rooms**

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

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.

1.1.2 Off-site storage

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

1. Approved Storage Facilities
CSI may only be stored in facilities authorized by University Administration.

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

1.2 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.

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

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.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Facility and Records Management Policy

Policy

Document Number: FCMN--102
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: VP of Administration
Status: Approved

General Description

Description: Where facilities have multiple users, consideration will be given to provide balance in use, which does not compromise the provision of programs and services to all constituents. The unique scheduling requirements of the users will be considered when allocating facilities, as well as provide fair access for participants. The University has no obligation to provide facilities for non-University users except where an explicit contract or agreement is provided.

Purpose: The students, faculty, staff, and administrators of Cumberland University share the physical facilities and athletic fields available to the University community. As such, these constituents rely on CU to provide facilities to offer quality facilities. Constituents enjoy participating in active and passive leisure and recognize the essential role that physical facilities play in the development of a healthy campus community. CU values the promotion and enhancement of a healthy, safe and active campus community by working in partnership to provide responsive, proactive, accessible and diverse programs and services. This requires the strategic use of all physical facilities to maximize University benefit(s).

Scope: All Departments and/or Department heads

Exceptions: **The following are exceptions to this policy:**
No exceptions

Responsibility: Administration

OBJECTIVES:

1. To provide safe and efficient operation/maintenance of facilities.
2. To ensure fair and equitable access to facilities for all users.
3. To provide support to groups offering programming on or around campus.
4. To work cooperatively with facility users to deliver quality programs and events.
5. To support facility development by fostering group development.
6. To maintain policies for appropriate use of University resources (leased, owned and/or controlled) in response to changing University needs.

Requirements

Approvals: All facility and records management questions must be referred to and approved by University administration.

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Policy Provisions

1. Priorities used for allocation

Facility allocation will be based on a simple priority sequence, which will be outlined hereto.

Organization + Activity = Priority

1. Providing space for classroom teaching and related academic activities.
2. Providing space for faculty, staff, and administrator offices.
3. University-operated programs and services.
4. Providing space for extracurricular functions including but not limited to athletics, music, arts, theatre, community, and other similar activities.
5. Providing space for residents on campus (residence halls, faculty or staff temporary housing).

2. Facility availability

Each of the University facilities has a schedule of availability based on the seasonal needs, maintenance requirements, and preferred hours of use, number of participants, and other requirements.

Effective Date: These Guidelines are considered to be in force as of June 1, 2011.

3. Guidelines

3.1 Guideline: Space Allocation, Facility Improvement, Facility Modifications, Facility Changes

Allocation of classroom, academic, residential, and individual office space is the responsibility of Vice President of Administration with final approval resting with the President of the University. Facility improvements, facility modifications, and facility changes are the responsibility of the Vice President of Administration with the final approval resting with the President of the University. ***No space allocation or facility improvement, modification, or change can take place without the approval of the President of the University.***

PURPOSE:
To insure that all University physical resources are allocated in a timely and fair manner. These Guidelines apply to all administrators, faculty, staff, and students of Cumberland University.

PROCEDURES/GUIDELINES:

1. Space allocation decisions will be made in response to hiring decisions (and the resulting office space need), the need for classroom space and/or adjustments to current classroom space, and/or the need for residential space for students. All space allocation decisions must be made by the President of the University upon consultation with and feedback provided by pertinent University administrators.
2. Immediately upon allocation of space for staff members, information regarding said space allocations will be forwarded to the appropriate unit to insure proper signage, electronic capability (telephone and computer access, etc.) and necessary changes to any University-wide communication system (telephone extension information, mailbox location, etc.). All space allocation needs are dependent on capital budget availability.
3. Written requests for space allocation adjustments/additions/needs will be considered by the Vice President of Administration only when an appropriate rationale is presented and requisite space is available. All space allocation decisions must be

approved by the President of the University. Furnishings and personal computers are part of the office and are not transferable unless otherwise noted in the written request. When changing offices, staff members are to move all of their personal effects, however all furnishings (desk, chair, bookcases, and standard computer) remain in the office they are vacating. Maintenance and Housekeeping is available to assist staff with moving heavy boxes. Specialized computer equipment required by staff members must be approved in the capital budget process. These computers may be moved with the staff from office to office only when written rationale is provided to Vice President of Administration. Once approved, Information Technology will arrange for this transfer of equipment. Individual staff members should not move their computer equipment. IT staff members will assist with moving computers.

4. Due to limited availability of office space, staff members will be limited to one office space per person. Efforts will be made to place instructional groups together when space is available. In some isolated cases, staff members may be asked to share office space, especially when work schedules allow (one staff member works daytime office hours and one staff member works night office hours).
5. Faculty office space will be allocated based on the following priority: Deans, Assistant Deans, administrative support, full-time faculty, and adjunct faculty (when space is available). Staff office space will be allocated based on the following priority: President, Administrators, administrative support, Directors of units, all other staff. Faculty and staff may be allocated a shared office space for the duration of his/her assignment. Larger offices may be assigned as shared office space when necessary. More than one faculty or staff member may be allocated to an office. Wherever possible, faculty and staff of the same department will be assigned shared office space.
6. It is the responsibility of the individual to ensure his/her office is cleared of all personal/ departmental belongings within one week of the end of his/her last day of employment.
7. When faculty members are granted a sabbatical or leave of absence, their office will be placed back into the office pool for the length of time they are away. It is the responsibility of the individual to ensure that the office is cleared of all personal/departmental belongings prior to leaving. In the event that a faculty member requires use of office space for the duration of his/her sabbatical/leave, a written request must be submitted to the Vice President of Administration. If there is office space available and the request is deemed appropriate by the Vice President of Administration, office space in the part-time suite may be appointed.
8. Classroom space allocations will be a collaborative process between the Registrar's office, the School Deans, the Vice President of Administration, the Office of Disability Services, and the Vice President of Administration. Final decision on classroom space allocation rests with the President of the University.
9. Residential space allocations will be a collaborative process between the Director of Residence Life and Housing, the Vice President of Administration, and the Executive Vice President. Final decision on residential space allocation rests with the President of the University.
10. Athletic department space allocation will be a collaborative process between the Director of Athletics (with input from pertinent coaches), the Vice President of Administration, the Office of Disability Services, and the Executive Vice President and CIEO. Final decisions on Athletic Department space allocation rest with the President of the University.
11. Any facility improvement, change, or modification must follow a collaborative process directed by the Vice President of Administration, and the final decision will rest with the President of the University. The process will include a written request for modification, a discussion by pertinent parties who will be involved, and approval by a line of administrators with the final decision resting with the President of the University. Included in this area:
    a. modification to any existing room, door, building, structure, or athletic field or facility;
    b. major or minor change to any existing room, door, building, structure, or athletic field or facility;
    c. facility expansion or renovation to any existing room, door, building, structure, or athletic field or facility;
    d. any cosmetic change to the campus interior or exterior (including removing trees, shrubbery, or signage or planting new trees, shrubs, or placing new signage on campus);

Any fundraising campaign with funds earmarked to improve, change, or modify any interior

or exterior site on campus must be approved prior to the campaign by the President of the University.

3.2 Guideline: Disposal of Records

To insure that all University records are handled in a secure manner. These Guidelines apply to all administrators, faculty, staff, and students of Cumberland University.

PROCEDURE/GUIDELINES

These guidelines set forth the procedures for disposal of institutional records for Cumberland University. Disposal of institutional records must be approved by the appropriate University administrator. No records may be destroyed unless and until provided below. Unless specified otherwise, or otherwise required by law, records may be imaged, microfilmed, or electronically reproduced and the paper copy destroyed upon verification of an archival quality reproduction. The microfilm, image, or electronic record will then be retained for the balance of the indicated retention period.

No record shall be destroyed so long as it pertains to any pending legal case, claim or action or to any federal or state audit until such actions have been concluded. Records which reflect "Permanent" retention may be destroyed after verification of an archival quality electronic reproduction.

Prior to the destruction of any records, the appropriate University administrator must determine if the action should be delayed due to audit or litigation requirements. Specific records pertaining to current or pending litigation or investigation must also be retained until the litigation is complete or legal counsel instructs that the records may be destroyed. These specific records can be retained in a suspense file, while all other records not under pending investigation should be disposed of in accordance with established procedures.

Notwithstanding the retention period stated herein, should such periods conflict with federal law, the period of longer retention shall apply. The following definitions are applicable to this Guideline:

RECORD: All books, papers, electronic mail messages, maps, photographs, films, microfilm, imaged copy, electronic data processing output, sound recordings or other materials regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any governmental agency.

NON-RECORD: Those documents which do not document the activities of the University: i.e. extra copies of documents kept for convenience or reference; stock supplies of publications; extra copies of circulated materials where follow-up copies are kept for the record; reading files; follow-up correspondence copies; identical or carbon copies kept in

the same file; draft copies or work copies of documents when the final version is complete; letters of transmittal which add nothing to the transmitted information; inter-office memoranda; shorthand notes, steno type tapes or sound recordings after they have been transcribed; and internal housekeeping materials such as intra-office memos, routing slips, telephone call slips, and computer edit error listings after the corrections are made; library or museum material which is for reference or exhibition; private materials neither made nor received by an institution or school staff member in connection with the transaction of official business. As non-records, the above-mentioned items are excluded from the record retention and disposal requirements.

PERMANENT RECORDS: Those records or materials which have permanent administrative, physical, historical or legal value.

WORKING PAPERS: Those records or materials created to serve as interim documents or inputs to final reporting documents, including electronic data processed records, computer output microfilm and records which become obsolete immediately after agency use or publication and are not classified as being a permanent record, or record of archival value.

3.2.1 Business records

NOTE: Business records must be retained the indicated number of years listed below.

TYPE OF RECORD	RETENTION PERIOD
Capital Outlay Requisitions	3 years
Capital Outlay Purchase Orders Closed capital outlay purchase order files	3 years
Requisition for Local Purchase	3 years
Requisition for Bids	3 years
Budget Records and Ledgers (Working Papers) Budget working papers which are prepared at each institution during the budget process	3 years
Travel Claims Claims for travel expenses filed for reimbursement	3 years
Purchase Orders	3 years
Petty Cash Receipts	3 years

Equipment Inventory Records	3 years
Disbursement Voucher Files Disbursement vouchers and supporting documents, such as vendor invoices, purchase orders and related correspondence, travel requests and authorizations	3 years
Motor Vehicle Operations Files Applications for title, registration, invoices, etc., for school-owned vehicles	3 years
Internal Audit Reports	5 years or two audits
Internal Audit Work Papers	5 years or two audits
Accounts Receivable Invoices billing individuals and organizations for accounts receivable	5 years
Bank Deposit Slips	5 years
University Operating Funds Receipt Books and Other Pre-Numbered Receipts	5 years
Payroll Records Payroll journals, transmittal sheets, etc.	4 years
Check Vouchers	5 years
Fee Assessment Forms	5 years
Vendor Files	5 years
Bank Account Reconciliation Statements showing checks, other debits, deposits and credits to bank accounts	5 years
Canceled Checks	5 years
Student Ledger Cards/ Student Registration System Receipts	5 years after account is paid in full; permanently if not paid in full

Tuition and Fee Charges, Assessed and Paid	5 years after date of charge
Investment Records Includes records concerning LGIP accounts, certificates of deposit, records of interest and dividends earned	5 years after maturity/liquidation of investment
Student Financial Aid Records 1. Records pertaining to the application for and receipt and expenditure of federal funds, including all accounting records and original and supporting documents necessary to document how the funds are spent 2. Records pertaining to specific award of financial aid 3. Repayment Records	A minimum of 3 years, as required by federal law. See 34 C.F.R. 668.24.
Contracts	6 years after either final payment, or termination of contract term
Housing Contracts	6 years after final payment
Leases	6 years after termination
Gift and Contribution Records Master listing of gifts and contributions Record of any stipulations placed on gift or contribution All other records	Permanently Life of gift or contribution 3 years
General Ledger	20 years
Monthly Budget and Expenditure Report (if different than General Ledger)	If kept in lieu of a general ledger, 20 years
Financial Reports	Permanently

3.2.2 Personnel records

NOTE: Personnel records must be retained the indicated number of years listed below.

TYPE OF RECORD	RETENTION PERIOD
Attendance and Leave Records, Employee Leave Requests, Attendance and Leave Reports	Maintain by fiscal year (current leave balances should be constantly maintained); hold for 3 years after current year and completed audit when required
Personnel Files Official personnel folders for each employee	Maintain in active files for current employees. May image, microfilm, or electronically reproduce active files; Destroy paper records after verification of reproduction.
Daily Work Report Files This record serves as a work sheet for the attendance and leave record. It serves as a record of daily attendance, hours worked and leave taken. Included are forms giving name of employee, time signed in and out, hours worked, signature of employee, etc.	Maintain in file on annual basis; destroy after maintaining 3 years
Pledge Cards for Charity Drives	Destroy after 1 year and audit
Employee Insurance Files Records consist of signed copies of group welfare program and similar forms indicating type coverage selected, signed application for health insurance and similar or related forms	Retain in active file until superseded by a new form, at which time original authorization will be placed in agency personnel folder or attached to the new authorization. Upon termination of employment, place in agency employee personnel folder, etc.
Applications for Employment Applications and resumes submitted in response to an advertised position.	2 years after date of last action on an application
Unsolicited Applications Employment applications and resumes gratuitously submitted.	May be disposed of immediately

Affirmative Action Records Composite information relating to applicant flow logs, applicant statistics, wage data, and information concerning adverse impact, affirmative action compliance program, etc.	5 years
I-9 Employment Eligibility verification forms	3 years after date of hire or one year after date of termination, whichever is later

3.2.3 Student records

The Family Educational Rights and Privacy Act of 1974, as amended (FERPA) specifically requires institutions to maintain records of requests and disclosures of personally identifiable information except for defined "directory information" and requests from students to review their own records. The records of disclosures and requests for disclosures are considered part of the students' educational records; therefore, these records must be retained as long as the education records to which they refer are retained by the institution.

Additionally, FERPA requires that no record for which there is a pending request to review be destroyed.

Admission data, documents for applicants who do not enter whether accepted or rejected.

TYPE OF RECORD	RETENTION PERIOD
Acceptance Letters	1 year after application term
Applications for Admission	1 year after application term
Correspondence	1 year after application term
Entrance Exam Reports (ACT, CEEB)	1 year after application term
Letters of Recommendation	1 year after application term
Transcripts High school, other colleges or universities	1 year after application term
Medical Records	1 year after application term

Readmission Forms	1 year after application term

The remainder of the retention guidelines for student records pertains to applicants who enter the institution.

TYPE OF RECORD	RETENTION PERIOD
Grade Reports (Registrar's copies)	1 year after date distributed
Registration Forms	1 year after date submitted
Social Security Certificates	1 year after certified
Teacher Certifications	1 year after certified
Transcript Requests (student)	1 year after date requested
Audit Authorizations	1 year after date submitted
Pass/Fail Requests	1 year after date submitted
Changes of Course (add/drop)	1 year after date submitted
Credit/No Credit Approvals	1 year after date submitted
Enrollment Verifications, Logs or Lists	1 year after date submitted
Applications for Graduation	1 year after graduation or 1 year after date of last attendance
Examination Papers and Answer Sheets	Must be retained one year after date of last attendance, or one year after date of graduation of student whose grade has been appealed.
Academic Advisor Files	1 year after graduation, or 3 years after end of advisor status, whichever occurs first

Class Schedules (Students)	1 year after graduation or 1 year after date of last attendance
Personal Data Information Forms	1 year after graduation or 1 year after date of last attendance
Judicial Board Cases/Student Disciplinary Files For matters resulting in expulsion or suspension For matters resulting in a finding of no violation(s)	Permanent At conclusion of disciplinary process
All other matters	1 year after graduation or 4 years after date of action
Veterans Administration Certifications/Individual Folders File includes recruitment material (for those who do not enter whether accepted or rejected); previous education (transcripts from other colleges); evidence of formal admission (acceptance letters); grade reports and/or statements of progress (academic records); change of course forms; transfer credit evaluations; degree audit reports; tuition and fees charged and collected.	3 years after graduation or date of last term attended
Withdrawal Authorizations	3 years after graduation or date of last attendance
Academic Action Authorizations (Dismissal, etc.)	5 years after graduation or date of last attendance
Acceptance Letters	5 years after graduation or date of last attendance
Name Change Authorizations	5 years after graduation or date of last attendance
Correspondence, Relevant	5 years after graduation or date of last attendance

Residence Classification Forms	5 years after graduation or date of last attendance
Curriculum Change Authorizations	5 years after graduation or date of last attendance
Degree Audit Records, Reports	5 years after graduation or date of last attendance
Entrance Examinations Reports (ACT, CEEB)	5 years after graduation or date of last attendance
Transcripts - High schools, other colleges	5 years after graduation or date of last attendance
Foreign Student Forms (I-20)	5 years after graduation or date of last attendance
Graduation Authorizations	5 years after graduation or date of last attendance
Advance Placement Records Information regarding students' high school advance placement scores	5 years after graduation or date of last attendance
Applications for Admission or Readmission (Re-entry)	5 years after graduation or date of last attendance
Credit by Examination Forms	5 years after graduation or date of last attendance
Placement Records Records of job placement subsequent to attendance, graduation, receipt of certificate, etc.	5 years after graduation or date of last attendance
Letters of Recommendation	Upon admission of the student
Student Waivers for Right of Access to Review Letters of Recommendation for Admission	Retain until the admissions record and recommendation letters are disposed.
Transfer Credit Evaluations	5 years after graduation or date of last attendance

Academic Records Includes Narrative Evaluations, Competency Assessments, etc.	Permanently
Change of Grade Forms (Update Forms)	Permanently
Class Lists (Original Grade Sheets or Cards)	Permanently
Graduation Lists	Permanently
Permanent Student Cards	Permanently
Statistical Data – Enrollment, Grades, Racial/Ethnic, Degree, Schedule of Classes (Institutional)	Permanently
Commencement Program	Retain 1 copy permanently

3.2.4 Miscellaneous

TYPE OF RECORD	RETENTION PERIOD
Correspondence Files	1 year
Deeds	Permanently
Endowment and Living Trust Agreements	Permanently
Minutes of Board and Committees Documents relating to the holding of meetings and recording of proceedings of meetings of the Board of Regents and its official commissions, councils, sub-councils, and committees. Included are accounts (either verbatim or in summary) of proceedings; actions taken in such meetings, agenda; copies of reports; exhibits; announcements; retained in Office of General Counsel	Permanently

Printed Materials and Publications Items which have permanent administrative, physical, historical or legal value, such as: Class schedules (institutional), school catalogs, brochures, etc.	Retain 2 copies permanently in institution/center library archive
Medical X-Rays	4 years, provided the written and signed findings of a radiologist who has read such X-ray film shall be retained for 10 years after treatment of patient
Medical Case Records	Retain entire record for 10 years after student leaves institution. Retain 10 years after treatment of member of institution/center staff
Litigation Files Institutional Files - Supporting records utilized in litigation Central Office Files - Pleadings and other supporting documents	3 years after conclusion of litigation/final appeal 5 years after conclusion of litigation/final appeal
Interlibrary Loan Forms	Maintain by calendar year and hold for 1 additional year
Motor Vehicle Registration Registration forms for campus parking permits	Retain during current academic year; or, destroy once invalid
Accreditation Records	Until superseded

3.3 Guideline: Business Continuity Plan (impact analysis, threat analysis, and recovery requirement

To insure that all University continues operation even in time of crisis.

These Guidelines apply to all administrators, faculty, staff, and students of Cumberland University.

3.3.1 Business impact analysis

The analysis phase in the development of the BCP consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

An impact analysis results in the differentiation between critical (urgent) and non-critical (non-urgent) organization functions/ activities. For each critical (in scope) function, two values are then assigned:

- Recovery Point Objective (RPO) - the acceptable latency of data that will be recovered
- Recovery Time Objective (RTO) - the acceptable amount of time to restore the function

The Recovery Point Objective must ensure that the Maximum Tolerable Data Loss for each activity is not exceeded. The Recovery Time Objective must ensure that the Maximum Tolerable Period of Disruption (MTPD) for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or

The technical requirements for recovery of the critical function

3.3.2 Threat analysis

The analysis phase in the development of the BCP consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

Some common threats include the following:

- Disease
- Earthquake
- Fire
- Flood
- Cyber attack
- Sabotage (insider or external tDirector of Human Resourceseat)
- Hurricane or other major storm
- Utility outage
- Terrorism
- Theft (insider or external threat, vital information or material)
- Random failure of mission-critical systems

All threats in the examples above share a common impact: the potential of damage to organizational infrastructure - except one (disease).

3.3.3 Recovery requirement documentation

The analysis phase in the development of the BCP consists of an impact analysis, threat analysis, and impact scenarios with the resulting BCP plan requirement documentation.

Business and technical plan requirements are documented in order to commence the implementation phase.

- The numbers and types of desks, whether dedicated or shared, required
- The individuals involved in the recovery effort along with their contact and technical details
- The applications and application data required for critical business functions
- The manual workaround solutions
- The maximum outage allowed for the applications

The peripheral requirements like printers, copier, fax machine, calculators, paper, pens, etc.

Performance Evaluation

Desired Outcome:

1. To provide safe & efficient operation/maintenance of facilities.
2. To ensure fair and equitable access to facilities for all users.
3. To provide support to groups offering programming on or around campus.
4. To work cooperatively with facility users to deliver quality programs and events.
5. To support facility development by fostering group development.
6. To maintain policies for appropriate use of University resources (leased, owned and/or controlled) in response to changing University needs.

Performance Metrics: Compliance with standard policy and procedure
Customer Satisfaction Rating

Consequences: Further training
Loss of privileges
Write-Up
Suspension
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Administration

VP of Business and Finance

Destruction

Policy

Document Number: REDFLAG--107
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about destruction of records relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. Destruction

1.1 Hard Copy Destruction

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

1.1.1 In-house storage awaiting sDirector of Human Resourcesedding

1. Is the responsibility of every department.
2. Hard copy material waiting to be shreded will be maintained in locked and secured boxes labeled “Confidential Shred Material.”

1.2 Destruction service providers

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

1.2.1 Destruction service providers

1. All destruction service providers must be National Association of Information Destruction, Inc. (NAID, Inc) Certified.
2. The University must be provided a certificate of destruction every time material is released to be destroyed.

1.3 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.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Transferability

Policy

Document Number: REDFLAG--108
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about transferability of information relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Standard company policies
Standards of good practice
State statutes
Local statutes

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. Transferability

1.1 Spoken Word

1. Company representatives must identify and verify callers as authorized before releasing any CSI over the phone.
2. Company representatives may not release any CSI to a third party unless the third party was previously authorized in writing.
3. Employees may only discuss CSI with University-authorized individuals for a legitimate business purpose.
4. Under no circumstances are company representatives permitted to leave CSI messages on voicemail systems.

1.2 Hard Copy Transferability

1. Clean Desk Policy
   - Company representatives shall keep desks and workspaces clear of CSI when not in use.

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.

3. Transporting Information
   - Confidential and Sensitive information shall be transported from one external location to another in the locked trunk of a vehicle.
   - An inventory must be kept of all CSI hard copy that is shipped.

4. Facsimiles (FAX)
   - 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.
   - Every outgoing fax must contain a cover sheet containing the senders and receivers names. Each coversheet will contain the University's Confidential and Sensitive Information Disclaimer.
   - Employees sending a FAX containing CSI shall notify the recipient that the FAX is being sent.
   - Any unnecessary CSI must be masked or deleted before faxing.

1.3 Soft Copy Transferability

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.

2. E-mail Transferability
   - All outgoing email containing CSI must be encrypted.
   - 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.

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.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Information Accessibility

Policy

Document Number: REDFLAG--109
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about information accessibility relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. Information Accessibility

1.1 Hard Copy Accessibility

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.

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.

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

4. Employee Authorization
   - Every employee will be thoroughly trained before being authorized to handle CSI.
   - Employees shall only handle CSI for a legitimate business purpose and that is a function of their job responsibilities.

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

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.

1.2 Soft Copy Accessibility

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

2. Logging on and off Computers
   - Only authorized personnel may log onto University networks and equipment.
   - All personnel are required to log off computers when not in use.

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.

4. Personal Use of Technology Equipment
   - Employees are permitted to browse the internet with company equipment only for company purposes.
   - Employees are permitted to instant message using company equipment only for company purposes.
   - Employees are permitted to check personal email on company equipment.

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

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Plan for a Loss or Breach

Policy

Document Number: REDFLAG--110
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about the plan for a loss or breach relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy and procedure.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. Plan for a Loss or Breach

1.1 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.

1.2 Discovery of a Breach in the Workplace

1. Employee Protocol
   - Do not disturb the area.
   - Secure the area.
   - Notify manager or supervisor.
   - Manager will contact Identity Theft Prevention Officer
   - Document the event.
   - Submit to Identity Theft Prevention Officer.

2. Manager or Supervisor Protocol
   - Ensure affected area is secure. Do not let anyone use the phone or computer in that area.

- Gather visitor logs, employee time sheets, list everyone who had access before, during, and after the incident.
- Interview employee witness(es).
- Contact ISO.
- Identity Theft Prevention Officer Protocol
- Determine that there is a breach
- Interview Employee Witness
- Review Security Incident Report
- Contact the University attorney
- Make a police report
- Notify potential victims according to legal statutes.
- Public relations and continuity considerations.

1.3 Discovery of a Breach Through Accusation

1. Employee Protocol
   - Be sympathetic to the potential victim
   - Do not confirm or deny their allegations
   - Document the conversation
   - Document contact information
   - Inform them that your Identity Theft Prevention Officer will contact them.
2. Identity Theft Prevention Officer Protocol
   - Interview Employee Witness
   - Review Security Incident Report
   - Contact potential victim.
   - Ask them to reiterate their story.
   - Assure them that you will look into it.
   - Contact your attorney.
   - Determine that there is a breach
   - Assess the extent of damage
   - Make a police report
   - Notify potential victims according to legal statutes.
   - Public relations and continuity considerations

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Suspicious Behavior

Policy

Document Number: REDFLAG--111
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about suspicious behavior relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility:
Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Loss of privilege, general

Policy Provisions

1. Suspicious Behavior
    1. University representatives shall document and confidentially report to senior management any suspicious behavior on behalf of other employees, customers, service providers, or visitors.
    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.

Performance Evaluation

Performance Metrics:
Compliance with standard policy and procedure
Compliance with federal mandate

Consequences:
Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Transaction Identification and Verification

Policy

Document Number: REDFLAG--112
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about transaction identification and verification relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy and procedure.

Scope: All faculty, staff, students, and administrators

Responsibility: Administration
Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice

Terms and Definitions: **Additional training**

Corrective Action

Loss of privilege, general

Policy Provisions

1. 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.

1.1 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.

1. US State Driver's License
2. US State Picture ID
3. US Passport
4. US Military ID
5. US Federal ID
6. Alien Registration Card
7. Physical Address
8. Phone Number
9. Valid Signature
10. Other

1.2 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.

1. US State Driver's License
2. US State Picture ID
3. US Passport
4. US Military ID
5. US Federal ID
6. Alien Registration Card
7. Physical Address
8. Credit / Debit Card Number
9. Expiration Date
10. CVC2 / CVV2 / CID
11. Valid Signature
12. Other

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Loss of privileges

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

New and Existing Account Identification and Verification

Policy

Document Number: REDFLAG--113
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about new and existing account information and verification relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Loss of privilege, general

Suspension

Termination

Policy Provisions

1. New and Existing Account Identification and Verification

1.1 New Accounts

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

1.1.1 Customer Identifying Information

1. Legal Name
2. Date of Birth
3. Physical Address
4. Social Security Number
5. EIN
6. Passport and Country of Issuance
7. Alien Identification Card Number
8. Power of Attorney
9. Other

1.1.2 Verification Documents

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

Primary Identification

1. US State Picture Driver's License
2. US State Picture Issued ID Card
3. US Passport
4. US Military Picture ID
5. Federal Picture ID
6. Alien Registration Card
7. Other

Secondary Identification

1. Social Security card
2. Individual taxpayer identification card
3. EIN
4. Voter registration, state of residence
5. Birth Certificate
6. Credit card
7. Bank cards
8. Insurance Cards
9. State government
10. Local government
11. Company identification
12. Police identification
13. Temporary Drivers Licence
14. US Federal Government issued Permanent Resident Card
15. US Federal Government issued Employment Authorization
16. Other

Alternative Documents for Elderly or Disabled

1. Utility Bill: telephone, electricity, gas, water.
2. Voters Registration
3. State issued birth certificate
4. Company retirement check payable to individual.
5. Federal or state or county benefit check issued to individual.
6. Court documents indicating custodian or fiduciary appointment
7. Social Security Card.
8. Individual Tax Identification Card
9. Other

Non-Document Verification

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

1. Credit report
2. Previous bank/credit union reference
3. Site visit
4. Telephone call to customer
5. Letter of Welcome
6. Public data base
7. Financial Statement
8. Professional papers

9. Certified articles of incorporation
10. Partnership agreement
11. Association resolution
12. Assumed name certificate
13. Trust agreement
14. Business license
15. Criminal Background Check
16. Medical Information Bureau (MIB) File
17. Other

1.2 Existing Accounts

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

1.2.1 Account Access in Person--Verification with Documents

Primary Identification

1. US State Picture Driver's License
2. US State Picture Issued ID Card
3. US Passport
4. US Military Picture ID
5. Federal Picture ID
6. Alien Registration Card
7. Other

Secondary Identification

1. Social Security card
2. Individual taxpayer identification card
3. EIN
4. Voter registration, state of residence
5. Birth Certificate
6. Credit card
7. Bank cards
8. Insurance Cards
9. State government
10. Local government
11. Company identification
12. Police identification
13. Temporary driver license
14. US Federal Government issued Permanent Resident Card
15. US Federal Government issued Employment Authorization
16. Other

Alternative Documents for Elderly or Disabled

1. Utility Bill: telephone, electricity, gas, water.
2. Voters Registration
3. Family Bible, on the "Birth" page the individual's name and date of birth
4. State issued birth certificate
5. Company retirement check payable to individual.
6. Federal or state or county benefit check issued to individual.
7. Court documents indicating custodian or fiduciary appointment
8. Social Security Card.
9. Individual Tax Identification Card
10. Other

1.2.2 Account Access On-line

Customer Identifying Information

1. Legal Name
2. Date of Birth
3. Physical Address
4. Account Number
5. Policy Number
6. Student Number
7. Social Security Number
8. EIN
9. Personal Identification Number
10. User ID
11. Password
12. Personal Knowledge Questions
13. Other

1.2.3 Account Access by Telephone

Customer Identifying Information

1. Legal Name
2. Date of Birth
3. Physical Address
4. Account Number
5. Policy Number
6. Student Number
7. Social Security Number
8. EIN
9. Personal Identification Number
10. User ID
11. Password
12. Email Address
13. Personal Knowledge Questions
14. Other

1.2.4 Account Access by Mail

Customer Identifying Information

1. Legal Name
2. Date of Birth
3. Physical Address
4. Account Number
5. Policy Number
6. Student Number
7. Social Security Number
8. EIN
9. Personal Identification Number
10. User ID
11. Password
12. Email Address
13. Personal Knowledge Questions
14. Letter of Instruction
15. Signature Guarantee
16. Notarization
17. Power of Attorney
18. Other

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Red Flags

Policy

Document Number: REDFLAG--114
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about red flags relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Fine

Loss of privilege, general

Termination

Policy Provisions

1. Red Flags

1.1 Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A customer reporting agency provides a notice of credit freeze in response to a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
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.
5. Other

1.2 Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
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.
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.
5. An application appears to be altered or forged, or gives the appearance of being reassembled.
6. Other

1.3 Suspicious Identifying Personal Information

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.
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.
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.
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.
5. The SSN provided is the same as that submitted by other persons.
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.
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.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
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.
10. Other

1.4 Unusual Use of Suspicious Activity Related to the Covered Account

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.
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.
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.

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

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

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.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Red Flags Response

Policy

Document Number: REDFLAG--115
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about the red flags response relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Loss of privilege, general

Termination

Policy Provisions

1. Red Flags Response

1.1 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:

1. Take additional steps to verify identity.
2. Flag relevant accounts.
3. Monitor account activity.
4. Decline account application.
5. Validate address.
6. Document with a Suspicious Activity Report (SAR).
7. Notify existing customer on record.
8. Other

1.2 Response to Suspicious Documents

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

1. Verify using third party resources.
2. Verify using existing account records.
3. Decline application.
4. Decline account access.
5. Document with a Suspicious Activity Report (SAR).
6. Notify law enforcement (if necessary)
7. Notify existing customer on record
8. Other

1.3 Response to Suspicious Identifying Personal Information

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

1. Escalate verification to a higher level.
2. Decline account application.
3. Decline account access.
4. Notify existing customer on record.
5. Change account access information.
6. Change account numbers.
7. Document with a Suspicious Activity Report (SAR).
8. Involve law enforcement.
9. Other

1.4 Response to Unusual Use of or 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:

1. Use Personal Knowledge questions for verification.
2. Validate address.
3. Decline account access.
4. Document with a Suspicious Activity Report (SAR).
5. Notify existing customer on record.
6. Change account access information.
7. Change account numbers.
8. Involve law enforcement.
9. Other

1.5 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:

1. Decline account access
2. Close fraudulent account
3. Document with a Suspicious Activity Report (SAR)
4. Notify existing customer on record
5. Open new account
6. Do Not Attempt to Collect on the Fraudulent Account from the True Identity
7. Cooperate with law enforcement
8. Other

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Staff Training

Policy

Document Number: REDFLAG--116
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about staff training relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Fine

Loss of privilege, general

Termination

Policy Provisions

1. Staff Training
    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 fulltime, on a periodic basis no less than once annually.
    2. Staff members will receive additional training triggered by changes in policy, changes in their mode of operations, security incidents, and new information.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Service Provider Oversight

Policy

Document Number: REDFLAG--117
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

General Description

Description: Information about service provider oversight relative to Red Flags Identity Theft Policy.

Purpose: Delineation of policy.

Scope: All faculty, staff, students, and administrators

Responsibility: Executive VP
VP of Business and Finance

Requirements

Relevant Knowledge: **In order to comply with this policy you should know:**
Current University policy
Federal statutes
Local statutes
Standard company policies
Standards of good practice
State statutes

Terms and Definitions:

Additional training

Corrective Action

Fine

Loss of privilege, general

Termination

Policy Provisions

1. Service Provider Oversight
    1. The University will periodically review all service provider agreements and activities no less than annually.
    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.
    3. A service provider that has indirect access to CSI shall comply with this Identity Theft Prevention Policy.

Performance Evaluation

Performance Metrics: Compliance with standard policy and procedure
Compliance with federal mandate

Consequences: Further training
Job Termination

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Purpose of Red Flags Identity Theft Policy

Info Sheet

Document Number: REDFLAG--100d
Revision #: 1.0
Document Owner: Executive VP
Date Last Updated: 08/17/2012
Primary Author: Executive VP
Status: Approved

List:

1. Purpose of the Red Flags Identity Theft Policy

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 tDirector of Human Resourceseats 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.

Subject Experts

The following may be consulted for additional information.

Executive VP

VP of Business and Finance

Regulations

federal mandate
Peer review standards
Standards of good practice
University governance