Revision Responsibility: IT Administrator
Responsible Executive Office: IT Department/Administration
Source/Reference: TBR Policy

PURPOSE

This policy is intended to provide a single, easily accessible and user-friendly document for students, employees, and others to inform them of the Information Technology resources available and the related responsibilities. TCAT Jacksboro encourages the use of mobile and portable devices in classrooms and throughout the institution. All devices attaching to TCAT Jacksboro's network is subject to monitoring. Devices found in violation of TCAT Jacksboro policies will be removed from the network because of copyright laws and for security.

POLICY

INTRODUCTION

Computer information systems and networks are an integral part of business at the Tennessee College of Applied Technology - Jacksboro. The institution has made a substantial investment in human and financial resources to create these systems. The enclosed policies and directives have been established in order to protect this investment, safeguard the information contained within these systems, reduce business and legal risk, and protect the good name of the Organization

VIOLATIONS

Violations may result in disciplinary action in accordance with school policy. Failure to observe these guidelines may result in disciplinary action by the organization, depending upon the type and severity of the violation, whether it causes any liability or loss to the institution, and/or the presence of any repeated violation(s).

ADMINISTRATION

The Information Systems Manager (IS Manager) is responsible for the administration of this policy.

CONTENTS

The topics covered in this document include:

1.) Information Technology Acceptable Use
2.) Personally Identifiable Information
3.) Password Management
4.) Identity Theft Prevention

Information Technology Acceptable Uses

Purpose

The objectives of this guideline include: 1) to articulate the rights and responsibilities of persons using information technology resources owned, leased, or administered by the Tennessee College of Applied Technology – Jacksboro; 2) to protect the interests of users and the Tennessee College of Applied Technology – Jacksboro; and 3) to facilitate the efficient operation of Tennessee College of Applied Technology – Jacksboro information technology systems.

Definitions

- Information technology resources or IT resources- include computers and computer time, data processing or storage functions, computer systems and services, servers, networks, printers and other input/output and connecting devices, and related computer records, programs, software, and documentation.
- Institution- shall mean the Tennessee College of Applied Technology – Jacksboro.
- Personal or private for-profit use - shall mean a use of Tennessee College of Applied Technology – Jacksboro information technology resources which has as a primary objective financial gain of the user. Activities by a student which are typical of the student job search process (e.g. use of campus e mail to contact potential employers or posting of one's resume on the Institution's website, if allowed under Institutional policies and procedures) are not to be considered personal or private for-profit uses.
- Public record - means all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, 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.

Guideline

1) User Responsibilities

The following lists of user responsibilities are intended to be illustrative, and not exhaustive.

a) Access Users shall obtain proper authorization before using Tennessee College of Applied Technology – Jacksboro information technology resources.
b) Users shall not use Tennessee College of Applied Technology – Jacksboro information technology resources for purposes beyond those for which they are authorized.
c) Users shall not share access privileges (account numbers and passwords) with persons who are not authorized to use them.
d) Users shall not use Tennessee College of Applied Technology – Jacksboro information technology resources in an attempt to access or to actually access computers external to the institution when that access is not authorized by the computer's owner (no "hacking" allowed).

2) Respect for others

a) A user shall not attempt to obstruct usage or deny access to other users.
b) Users shall not transmit or distribute material that would be in violation of existing Tennessee College of Applied Technology – Jacksboro policies or guidelines using Tennessee College of Applied Technology – Jacksboro information technology resources.
c) Users shall respect the privacy of other users, and specifically shall not read, delete, copy, or modify another user's data, information, files, e-mail or programs (collectively, "electronic files") without the other user's permission.

Users should note that there should be no expectation of privacy in electronic files stored on the resident memory of a computer available for general public access, and such files are subject to unannounced deletion.

d) Users shall not intentionally introduce any program or data intended to disrupt normal operations (e.g. a computer "virus" or "worm") into Tennessee College of Applied Technology – Jacksboro information technology resources.
   i) Forgery or attempted forgery of e-mail messages is prohibited.
   ii) Sending or attempts to send unsolicited junk mail or chain letters is prohibited.
   iii) Flooding or attempts to flood a user's mailbox is prohibited.

3) Respect for State-owned property

a) A user shall not intentionally, recklessly, or negligently misuse, damage or vandalize Tennessee College of Applied Technology – Jacksboro information technology resources.
b) A user shall not attempt to modify Tennessee College of Applied Technology – Jacksboro information technology resources without authorization.
c) A user shall not circumvent or attempt to circumvent normal resource limits, logon procedures, or security regulations.
d) A user shall not use Tennessee College of Applied Technology – Jacksboro information technology resources for purposes other than those for which they were intended or authorized.
e) A user shall not use Tennessee College of Applied Technology – Jacksboro information technology resources for any private or personal for-profit activity.
f) Except for those not-for-profit business activities which are directly related to an employee's job responsibilities or which are directly related to an organization which is affiliated with the Institution, a user shall not use Tennessee College of Applied Technology – Jacksboro information technology resources for any not-for-profit business activities, unless authorized by the Director (or his/her designee).
g) Users shall at all times endeavor to use Tennessee College of Applied Technology – Jacksboro information technology resources in an efficient and productive manner, and shall specifically avoid excessive game playing, printing excessive copies of documents, files, data, or programs; or attempting to crash or tie-up computer resources.

4) Additional Responsibilities of Employees and Independent Contractors

a) Users who are Employees and Independent Contractors shall not make use of Tennessee College of Applied Technology – Jacksboro information technology resources for purposes which do not conform to the purpose, goals, and mission of the Tennessee College of Applied Technology – Jacksboro and to the user's job duties and responsibilities.
b) Users shall not use Tennessee College of Applied Technology – Jacksboro information technology resources for solicitation for religious or political causes.

5) Digital/Electronic Signatures and Transactions

a) The Tennessee Board of Regents and its institutions must comply with the Tennessee Uniform Electronic Transactions Act (T.C.A. §47-10-101 et seq.) This Act permits the use of electronic signatures and electronic transactions under certain circumstances.
b) In order to be legally enforceable, an electronic signature must meet the following two criteria.
c) An electronic signature must be attributable (or traceable) to a person who has the intent to sign the record or contract with the use of adequate security and authentication measures that are contained in the method of capturing the electronic transaction.
   d) The recipient of the transaction must be able to print or store the electronic record of the transaction at the time of receipt. (T.C.A. §47-10- 109).

e) The use of electronic/digital signatures in compliance with state and federal laws is permitted.

6) No Unlawful Uses Permitted

a) Users shall not engage in unlawful uses of the information technology system resources of the Tennessee College of Applied Technology – Jacksboro.
b) Unlawful activities are volatile of this guideline and may also subject persons engaging in these activities to civil and/or criminal penalties.
c) This list of unlawful activities is illustrative and not intended to be exhaustive.

(1) Obscene Materials
   (a) The distribution and display of obscene materials is prohibited by the laws of Tennessee (seeT.C.A.39-17-902). Obscene materials are defined under Tennessee law (see T.C.A.39-17-901(10)) as those materials which:
   (b) The average person applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest;
   (c) The average person applying contemporary community standards would find that the work depicts or describes, in a patently offensive way, sexual conduct; and
   (d) The work, taken as a whole, lacks serious literary, artistic, political, or scientific value.
   (e) Federal law (18U.S.C.2252) prohibits the distribution across state lines of child pornography.

(2) Defamation - Defamation is a civil tort which occurs when one, without privilege, publishes false and defamatory statements which damage the reputation of another.

(3) Violation of Copyright

   (a) Federal law gives the holder of copyright five exclusive rights, including the right to exclude others from reproducing the copyrighted work.
   (b) Sanctions for violation of copyright can be very substantial. Beyond the threat of legally imposed sanctions, violation of copyright is an unethical appropriation of the fruits of another's labor.

(4) Gambling - Gambling, including that performed with the aid of the Internet, is prohibited under Tennessee state law (see T.C.A. § 39-17-502).

7) Tennessee College of Applied Technology – Jacksboro Monitoring and Inspection of Electronic Records

a) Electronic records sent, received, or stored on computers owned, leased, or administered by the Tennessee College of Applied Technology – Jacksboro is the property of the Tennessee College of Applied Technology – Jacksboro.
b) As the property of the Tennessee College of Applied Technology – Jacksboro, the content of such records, including electronic mail, is subject to inspection by Tennessee College of Applied Technology – Jacksboro personnel.
c) While the Tennessee College of Applied Technology – Jacksboro does not routinely do so, the Tennessee College of Applied Technology – Jacksboro is able and reserves the right to monitor and/or log all network activity of users without notice, including all email and Internet communications.
d) Users should have no reasonable expectation of privacy in the use of these resources.

8) Disclosure of Electronic Records

a) Pursuant to T.C.A. § 10-7-101 et sq., and subject to exemptions contained therein, electronic files (including email correspondence) may be subject to public inspection upon request by a citizen of the State of Tennessee, if they are:
   (1) Generated or received by TBR employees, and
   (2) Either owned or controlled by the State, or
   (3) Maintained using TBR IT resources.

b) Tennessee College of Applied Technology – Jacksboro personnel receiving such a request for public inspection should refer the request to the Director of Tennessee College of Applied Technology – Jacksboro.
c) Institutions may charge reasonable fees for making copies of such records, pursuant toT.C.A. §10-7-506.
d) While disclosure under T.C.A. § 10-7-101 et sq. applies to employees, disclosure of the electronic records of all users which are maintained using Tennessee College of Applied Technology – Jacksboro IT resources may be made pursuant to a valid subpoena or court order, when otherwise required by federal, state or local law, or when authorized by the President or Director of the Institution.

9) Retention of Electronic Records

a) Electronic records needed to support Institutional functions must be retained, managed, and made accessible in record-keeping or filing systems in accordance with established records disposition authorizations approved by the Public Records Commission and in accordance with TBR Guideline G-070, "Disposal of Records".
b) Each employee of the Tennessee College of Applied Technology – Jacksboro, with the assistance of his or her supervisor as needed, is responsible for ascertaining the disposition requirements for those electronic records in his or her custody.
c) The system administrator is not responsible for meeting the record retention requirements established under T.C.A. § 10-7-101 et sq., and the Tennessee College of Applied Technology – Jacksboro, as owner of electronic records stored on Tennessee College of Applied Technology – Jacksboro computers, reserves the right to periodically purge electronic records, including email messages.
d) Users who are either required to retain an electronic record, or who otherwise wish to maintain an electronic record should either:
   (a) Print and store a paper copy of the record in the relevant subject matter file; or
   (b) Electronically store the record on a storage medium or in an electronic storage location not subject to unannounced deletion.

10) Violation of this Guideline

a) Reporting Allegation of Violations

   (1) Persons who have reason to suspect a violation of this guideline, or who have direct knowledge of behavior in violation of this guideline should report that allegation of violation to the Director or his/her designee.

b) Disciplinary Procedures

(1) Allegations of violation of this guideline shall be referred by the designee of the Director to the appropriate person(s) for disciplinary action.
(2) If a student, the guideline violation will be referred to the judicial officer of the institution under TBR Policy 3:02:00:01.
(3) If an employee, the guideline violation will be referred to the immediate supervisor.
(4) If there is a guideline violation, which the designee believes rises to the level of a serious violation of this or any other TBR policy/guideline; the designee is authorized to temporarily revoke access privileges. In those cases, the revocation of access must be reviewed by the appropriate disciplinary authority for review and final determination of access privileges. In such cases the authorization of the designee carries with it the authorization to make subjective judgments, such as whether material or statements violate TBR Policy/Guideline.

11) Sanctions

a) Persons violating this guideline are subject to revocation or suspension of access privileges to Tennessee College of Applied Technology – Jacksboro IT resources.
b) Additionally other penalties, as outlined in TBR Policy 3:02:00:01 may be imposed upon student users.
c) Sanctions for violation of this guideline by employees may extend to termination of employment. Violations of law may be referred for criminal or civil action.

12) Appeals

a) Sanctions imposed upon students at a Tennessee College of Applied Technology – Jacksboro imposed at the discretion of the senior IT officer may be appealed to the Chief Student Affairs Officer.
b) Other sanctions may be appealed under established Institution procedure.

Personally Identifiable Information (PII)

Tennessee College of Applied Technology – Jacksboro creates, collects, maintains, uses, and transmits personally identifiable information relating to individuals associated with the institution including, but not limited to, students, alumni, faculty, administrators, staff, and service employees. The institution is committed to protecting PII against inappropriate access and use in compliance with applicable laws and regulations in order to maximize trust and integrity.

Definitions

- Data Custodians: Data Custodians are institutional designees who have planning and policy-making responsibilities for institutional data and the institutional Data Warehouse. The Data Custodians, as a group, are responsible for overseeing the establishment of data management policies and procedures and for the assignment of data management accountability.
- Minimum Necessary: Minimum Necessary is the standard that defines that the least information and fewest people should be involved to satisfactorily perform a particular function.
- Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, or biometric records, alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.
- Directory information: Directory Information is determined by each institution and is not considered PII.

1) Guideline

a) Members of the Tennessee College of Applied Technology – Jacksboro faculty shall employ reasonable and appropriate administrative, technical, and physical safeguards to protect the integrity, confidentiality, and security of all personally identifiable information (PII), irrespective of its source or ownership or the medium used to store it.
b) All individuals who dispense, receive, and store PII have responsibilities to safeguard it.
c) In adopting this policy, the Institution is guided by the following objectives:
   i) To enhance individual privacy for members of the Tennessee College of Applied Technology – Jacksboro community through the secure handling of PII and personal identifiers (PIDs);
   ii) To ensure that all members of the Tennessee College of Applied Technology – Jacksboro community understand their obligations and individual responsibilities under this policy by providing appropriate training that will permit the Tennessee College of Applied Technology – Jacksboro community to comply with both the letter and the spirit of all applicable privacy legislation. Each member institution will be responsible for determining the means of training for its institution;
   iii) To increase security and management of Social Security numbers (SSNs) by:
      (1) Instilling broad awareness of the confidential nature of the SSNs;
      (2) Establishing a consistent policy about the use of SSNs throughout the System; and
      (3) Ensuring that access to SSNs for the purpose of conducting TBR business is granted only to the extent necessary to accomplish a given task or purpose.
      (4) To reduce reliance on the SSN for identification purposes as much as possible.
   iv) To comply with all Payment Card Industry (PCI) standards
   v) To comply with HIPPA standards (if applicable)
d) Data Custodians are responsible for oversight of personally identifiable information in their respective areas of institutional operations. Activities of these officials are aligned and integrated through appropriate coordination among these cognizant institutional officials.

2) Scope

This policy applies to all members of the Tennessee College of Applied Technology – Jacksboro community, including all full- and part-time employees, faculty, students and their parents or guardians, and other individuals such as contractors, consultants, other agents of the community, alumni, and affiliates that are associated with the System or whose work gives them custodial responsibilities for PII.

3) Guideline Requirements

a) Data Trustees
   i) Officials responsible for each of the following areas will be considered data custodians:
      (1) Student Records
      (2) Alumni and Donor Records
      (3) Health Records
      (4) Faculty and Staff Records
      (5) Purchasing and Contracts
      (6) Research Subjects
      (7) Public Safety

4) Personally Identifiable Information

a) PII may be released only on a Minimum Necessary basis and only to those individuals who are authorized to use such information as part of their official TBR duties, subject to the requirements:
   i) That the PII released is narrowly tailored to a specific business requirement;
   ii) That the information is kept secure and used only for the specific official Tennessee College of Applied Technology – Jacksboro [business] purposes for which authorization was obtained; and
   iii) That the PII is not further disclosed or provided to others without proper authorization as defined above.
b) PII may be handled by third parties with the strict requirement that the information be kept secure and used only for a specific official authorized business purpose as defined in a Business Associate Agreement with that third party.
c) Exceptions to this policy may be made only upon specific requests approved by the cognizant institutional official responsible for such information as specified in this policy and only to the degree necessary to achieve the mission and business needs of the institution.
   i) Any and all exceptions made must be documented, retained securely, and reviewed periodically by the appropriate cognizant institutional official or his/her designee.
d) Directory Information, as defined by Federal and State law and institutional policy, will be published following the guidelines defined by the institution.
e) Information that has been collected that conforms to the HIPAA standards of deidentification or anonymization is not PII.

5) Government-Issued Personal Identifiers

a) Social Security Number

i) Provision of Information
(1) Tennessee College of Applied Technology – Jacksboro collect SSNs:
(a) When required to do so by law;
(b) When no other identifier serves the business purpose; and
(c) When an individual volunteers the SSN as a means of locating or confirming personal records.
(2) In other circumstances, individuals are not required to provide their SSN verbally or in writing at any point of service, nor are they to be denied access to those services should they refuse to provide an SSN.

ii) Release of SSNs
(1) SNs will be released to persons or entities outside the institution only:
(a) As required by law;
(b) When permission is granted by the individual;
(c) When the external entity is acting as the institution's authorized contractor or agent and attests that no other methods of identification are available, and reasonable security measures are in place to prevent unauthorized dissemination of SSNs to third parties; or
(d) When the appropriate Counsel has approved the release.

iii) Use, Display, Storage, Retention, and Disposal
(1) SSNs or any portion thereof will not be used to identify individuals except as required by law or with approval by a cognizant Tennessee College of Applied Technology – Jacksboro official for Tennessee College of Applied Technology – Jacksboro business purpose.
(2) The release or posting of personal information, such as grades or occupational listings, keyed by the SSN or any portion thereof, is prohibited, as is placement of the SSN in files with unrestricted access.
(3) SSNs will be transmitted electronically only for business purposes approved by the institutional officials responsible for SSN oversight and only through secure mechanisms.
(4) The Data Custodians who are responsible for SSNs will oversee the establishment of business rules for the use, display, storage, retention, and disposal of any document, item, file, or database which contains SSNs in print or electronic form.

b) Non-SSN Government-Issued Identifiers
i) In the course of its business operations, Tennessee College of Applied Technology – Jacksboro have access to, collect, and use non-SSN government-issued identifiers such as driver's licenses, passports, HIPAA National Provider Identifiers, Employee Identification Numbers (EIN), and military identification cards, among others.
ii) Tennessee College of Applied Technology – Jacksboro shall follow the Minimum Necessary standard and strive to safeguard these identifiers.

6) TBR Institution-Issued Identifiers

a) Institutional ID Number
i) Assignment Eligibility and Issuance
(1) The institutional id is a unique alphanumeric identifier assigned by the institution to any entity that requires an identifying number in any institutional system or record.
(2) An Institutional ID is assigned at the earliest possible point of contact between the entity and the institution.
(3) The Institutional ID is associated permanently and uniquely with the entity to which it is assigned.
ii) Use, Display, Storage, Retention, and Disposal

(1) The Institutional ID is considered PII by the institution, to be used only for appropriate business purposes in support of operations.

(2) The Institutional ID is used to identify, track, and serve individuals across all institutional electronic and paper data systems, applications, and business processes throughout the span of an individual's association with the institution and presence in the institution's systems or records.
(3) The Institutional ID is not to be disclosed or displayed publicly by the Institution, nor to be posted on the institution's electronic information or data systems unless the Institutional ID is protected by access controls that limit access to properly authorized individuals.
(4) The release or posting of personal information keyed by the Institutional ID, such as grades, is prohibited.
(5) Any document, item, file, or database that contains Institutional IDs in print or electronic form is to be protected and disposed of in a secure manner in compliance with data retention rules.

7) Other Externally-Assigned Identifiers and Other Personally Identifiable Information

Tennessee College of Applied Technology – Jacksboro shall follow the Minimum Necessary standard and strive to safeguard any externally assigned identifiers which may be collected.

8) Responsibility for Maintenance and Access Control

a) Institutional IDs are maintained and administered by the appropriate office in accordance with this policy.
b) Other institutional offices may maintain and administer electronic and physical repositories containing personal identification numbers for uses in accordance with this policy.
c) Access to electronic and physical repositories containing PII will be controlled based upon reasonable and appropriate administrative, physical, technical, and organizational safeguards.
d) Individuals who inadvertently gain access to a file or database containing PII should report it to the appropriate authority.

9) Enforcement

Violations of this policy resulting in misuse of, unauthorized access to, or unauthorized disclosure or distribution of personal identification numbers may subject individuals to legal and/or disciplinary action, up to and including the termination of employment or contract with the Institution or, in the case of students, suspension or expulsion from the institution.

Password Management

Purpose

The purpose of this guideline is to establish a minimum expectation with respect to password construct in order to protect data stored on computer systems throughout the system.

Guideline

1) Policy

a) A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access institutional networks and systems.
b) Passwords will be used for authentication of access to all institutional network and systems except where stronger authentication methods (such as biometric authentication or two-factor authentication) are deemed necessary.
c) The effectiveness of passwords to protect access to the institution's information directly depends on strong construction and handling practices.

2) Password Construction

a) All users must construct strong passwords for access to all institution networks and systems, using the following criteria where technically feasible:
   i) Must be a minimum of 8 characters in length.
   ii) Must be composed of a combination of at least three of the following four types of characters:
      (1) Upper case alphabetic character;
      (2) Lower case alphabetic character;
      (3) Numeric character;
      (4) Non-alphanumeric character
   iii) Or, as an alternative:
      (1) A passphrase of a minimum of 14 characters.

3) Password Management

a) The following requirements apply to end-user password management.
   i) Storage and Visibility
      (1) Passwords must not be stored in a manner which allows unauthorized access.

(2) Passwords will not be stored in a clear text file.
(3) Passwords will not be sent via unencrypted e-mail.

ii) Changing Passwords
(1) Users must change their passwords at least every 365 days.
(a) Student accounts are excepted from this requirement.
(2) Users who process or access restricted data (such as protected health information, student FERPA data, and Social Security Numbers or other personally identifiable information) should change their passwords at least every 120 days.
(3) Users with privileged accounts (such as those with root or administrator level access) must change their passwords at least every 120 days.
(4) Passwords must be changed immediately if any of the following events occur:
(a) Unauthorized password discovery or usage by another person;
(b) System compromise (unauthorized access to a system or account);
(c) Insecure transmission of a password;
(d) Accidental disclosure of a password to an unauthorized person; or
(e) Status changes for personnel with access to privileged and/or system accounts.

4) Password Protection – System Accounts

a) System Accounts can be defined as:
i) Accounts used for automated processes without user interaction.
ii) Accounts used for device management.
b) System Accounts are not required to expire but must meet the password construction requirements above.
c) Vendor provided passwords must be changed upon installation using the password construction requirements above.

5) Compliance and Enforcement

a) The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users.
b) Persons in violation of this policy are subject to a range of sanctions determined and enforced by the individual institutions.
c) Justifications for exceptions to this policy must be documented by the institution.

Identity Theft Prevention

Purpose

Tennessee College of Applied Technology – Jacksboro adopts this Identity Theft Prevention Policy and enacts this program in an effort to detect, prevent and mitigate identity theft, and to help protect the Institutions, their faculty, staff, students and other applicable constituents from damages related to the loss or misuse of identifying information due to identity theft.

Definitions

- Covered account - includes:
  - Any account that involves or is designated to permit multiple payments or transactions; or
  - Any other account maintained by the Institution for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the Institution from identity theft, including financial, operational, compliance, reputation or litigation risks.
- Identifying information - is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer Internet Protocol address or routing code, credit card number or other credit card information.
- Identity theft - means a fraud committed or attempted using the identifying information of another person without authority.
- Red flag - is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Policy

1) Background

a) The risk to the institutions of the Tennessee College of Applied Technology – Jacksboro, its faculty, staff, students and other applicable constituents from data loss and identity theft is of significant concern to the Board and its Institutions, and the Institutions should make reasonable efforts to detect, prevent, and mitigate identity theft.

b) Under this Policy the program will:
   i) Identify patterns, practices or specific activities ("red flags") that could indicate the existence of identity theft with regard to new or existing covered accounts (see Definitions);
   ii) Detect red flags that are incorporated in the program;
   iii) Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft;
   iv) Ensure periodic updating of the program, including reviewing the accounts that are covered and the identified red flags that are part of this program; and,
   v) Promote compliance with state and federal laws and regulations regarding identity theft protection.

c) The program shall, as appropriate, incorporate existing TBR and institutional policies and guidelines such as anti-fraud programs and information security programs that establish controls for reasonably foreseeable risks.

2) Identification of Red Flags

a) The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification.

b) Alerts, notifications or warnings from a credit or consumer reporting agency. Examples of these red flags include the following:
   i) A report of fraud or active duty alert in a credit or consumer report;
   ii) A notice of credit freeze from a credit or consumer reporting agency in response to a request for a credit or consumer report;
   iii) A notice of address discrepancy in response to a credit or consumer report request; and,
   iv) A credit or consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant such as:
      (1) A recent and significant increase in the volume of inquiries;
      (2) An unusual number of recently established credit relationships;
      (3) A material change in the use of credit, especially with respect to recently established credit relationships; or,
      (4) An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

c) Suspicious documents. Examples of these red flags include the following:
   i) Documents provided for identification that appears to have been altered, forged or are inauthentic.
   ii) The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
   iii) Other information on the identification is not consistent with information provided by the person opening a new covered account or individual presenting the identification.
   iv) Other information on the identification is not consistent with readily accessible information that is on file with the Institution, such as a signature card or a recent check.
   v) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

d) Suspicious personal identifying information. Examples of these red flags include the following:
   i) Personal identifying information provided is inconsistent when compared against other sources of information used by the Institution. For example:
      (1) The address does not match any address in the consumer report; or,
      (2) The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
   ii) Personal identifying information provided by the individual is not consistent with other personal identifying information provided by that individual. For example:
      (1) There is a lack of correlation between the SSN range and date of birth.
   iii) Personal identifying information provided is associated with known fraudulent activity. For example:
      (1) The address on an application is the same as the address provided on a fraudulent application; or,
      (2) The phone number on an application is the same as the number provided on a fraudulent application.
   iv) Personal identifying information provided is of a type commonly associated with fraudulent activity. For example:

(1) The address on an application is fictitious, a mail drop, or a prison; or
(2) The phone number is invalid or is associated with a pager or answering service.

v) The social security number provided is the same as that submitted by another person opening an account.
vi) The address or telephone number provided is the same as or similar to the address or telephone number submitted by that of another person.

vii) The individual opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
viii) Personal identifying information provided is not consistent with personal identifying information that is on file with the Institution.
ix) When using security questions (mother's maiden name, pet's name, etc.), the person opening that covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

e) Unusual use of, or suspicious activity related to, the covered account. Examples of these red flags include the following:
i) Shortly following the notice of a change of address for a covered account, the Institution receives a request for a new, additional, or replacement card, or for the addition of authorized users on the account.
ii) A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
(1) Nonpayment when there is no history of late or missed payments;
(2) A material change in purchasing or usage patterns.
iii) 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).
iv) Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
v) The Institution is notified that the individual is not receiving paper account statements.
vi) The Institution is notified of unauthorized charges or transactions in connection with an individual's covered account.
vii) The Institution receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the Institution.
viii) The Institution is notified by an employee or student, 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.
ix) A breach in the Institution's computer security system.

3) Detecting Red Flags

a) Student enrollment. In order to detect red flags associated with the enrollment of a student, the Institution will take the following steps to obtain and verify the identity of the individual opening the account:
i) Require certain identifying information such as name, date of birth, academic records, home address or other identification; and,
ii) Verify the student's identity at the time of issuance of the student identification card through review of driver's license or other government-issued photo identification.

b) Existing accounts. In order to detect red flags associated with an existing account, the Institution will take the following steps to monitor transactions on an account:
i) Verify the identification of students if they request Information;
ii) Verify the validity of requests to change billing addresses by mail or email, and provide the student a reasonable means of promptly reporting incorrect billing address changes; and,
iii) Verify changes in banking information given for billing and payment purposes.

c) Consumer/Credit Report Requests. In order to detect red flags for an employment or volunteer position for which a credit or background report is sought, the Institution will take the following steps to assist in identifying address discrepancies:
   i) Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
   ii) In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the Institution has reasonably confirmed is accurate.

4) Responding to Red Flags

a) Once a red flag or potential red flag is detected, the Institution must act quickly with consideration of the risk posed by the red flag.
b) The Institution should quickly gather all related documentation, write a description of the situation and present this information to the Program Administrator for determination.
c) The Program Administrator (see Section VI) will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
d) The Institution may take the following steps as is deemed appropriate:
   i) Continue to monitor the covered account for evidence of identity theft;
   ii) Contact the student or applicant for which a credit report was run;
   iii) Change any passwords or other security devices that permit access to covered accounts;
   iv) Close and reopen the account;
   v) Determine not to open a new covered account;
   vi) Provide the student with a new student identification number;
   vii) Notify law enforcement;
   viii) Determine that no response is warranted under the particular circumstances;
   ix) Cancel the transaction.

5) Protecting Personal Information

a) In order to prevent the likelihood of identity theft occurring with respect to covered accounts, the Institutions may take the following steps with respect to its internal operating procedures:
   i) Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
   ii) Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
   iii) Clear desks, workstations, work areas, printers and fax machines, and common shared work areas of all documents containing covered account information when not in use.
   iv) Documents or computer files containing covered account information will be destroyed in a secure manner. Institution records may only be destroyed in accordance with the Board's records retention guideline, TBR Guideline G-070 Disposal of Records.
   v) Ensure that office computers with access to covered account information are password protected.
   vi) Ensure that computer virus protection is up to date.
   vii) Avoid the use of social security numbers.
   viii) Utilize encryption devices when transmitting covered account information.
b) Institutional personnel are encouraged to use common sense judgment in securing covered account information to the proper extent.

c) Furthermore, this section should be read in conjunction with the Family Education Rights and Privacy Act ("FERPA"), the Tennessee Public Records Act, and other applicable laws and policies.

d) If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor. The Office of the General Counsel may be contacted for advice.

6) Program Administration

a) Oversight and Appointment of the Institutional Program Administrator
   i) The Identity Theft Prevention Policy is the responsibility of the governing body, the Tennessee Board of Regents. Approval of the initial plan must be appropriately documented and maintained.
   ii) Each individual institution is required to tailor this program taking into consideration its size, complexity, and nature of its operation. Each institution will consider the types of accounts it offers and maintains, the methods it provides to open those accounts, the methods it provides to access its accounts and its previous experience with identity theft.
   iii) Operational responsibility of the program at each individual institution is delegated to a Program Administrator appointed by the President or Director and shall include but not be limited to;
      (1) The oversight, development, implementation and administration of the program;
      (2) Approval and implementation of needed changes to the program; and,
      (3) Staff training.
   iv) The Program Administrator is also responsible for ensuring that appropriate steps are taken for preventing and mitigating identity theft, for reviewing any staff reports regarding the detection of red flags, and for determining which steps should be taken in particular circumstances when red flags are suspected or detected.
   v) A report to the Director should be made annually concerning institutional compliance with and effectiveness of the program, and the responsibility for such report may be placed with the Program Administrators. This report should address;
      (1) Service provider arrangements;
      (2) The effectiveness of the program in addressing the risk of identity theft;
      (3) Significant incidents of identity theft and the institution's response; and,
      (4) Any recommendations for material changes to the program.

b) Staff training
   i) Staff training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the Program Administrator, that may come into contact with covered accounts or identifying information.

c) Periodic Updates to the Program
   i) At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable.
   ii) Consideration will be given to the Institution's;
      (1) Experiences with identity theft situations;
      (2) Changes in identity theft methods, detection methods or prevention methods; and,
      (3) Changes in the Institution's business arrangements with other entities.
   iii) Periodic reviews will include an assessment of which accounts are covered by the program.
      (1) As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.
   iv) Actions to take in the event that fraudulent activity is suspected or discovered may also require revision to the program.

d) Overview of service provider arrangements

i) It is the responsibility of the Institution to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designated to detect, prevent, and mitigate the risk of identity theft.

ii) In the event the Institution engages a service provider to perform an activity in connection with one or more covered accounts, the Institution will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.
   (1) Require, by contract, that service providers have such policies and procedures in place; or,
   (2) Require, by contract, that service providers review the Institution's program and report any red flags to the Program Administrator.
      (a) Specific language for inclusion in contracts can be found in TBR Guideline G-030 Contracts and Agreements.

iii) A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.