TENNESSEE COLLEGE OF APPLIED TECHNOLOGY
McMINNVILLE

McMinnville Campus

Information Technology Policies

241 Vo-Tech Drive
McMinnville, TN 37110
Phone (931) 473-5587
Fax (931) 473-6380

The IT and Security Policy contained within are available on the TCAT McMinnville.edu Website.

Table of Contents

Mission Statement

The Tennessee Colleges of Applied Technology serve as the premier providers for workforce development throughout the State of Tennessee. The Colleges fulfill their mission by:

- Providing competency-based training through superior quality, traditional and distance learning instruction methods that qualify completers for employment and job advancement;
- Contributing to the economic and community development of the communities served by training and retraining employed workers;
- Ensuring that programs and services are economical and accessible to all residents of Tennessee; and
- Building relationships of trust with community, business, and industry leaders to supply highly skilled workers in areas of need.

Introduction

The Tennessee College of Applied Technology - McMinnville is a modern training facility designed to simulate the occupational environment found in places of employment. The primary purpose of the institution is to meet more adequately the occupational and technical training needs of citizens and residents of the institution's service area; these include employees of existing or prospective industries and businesses.

TCAT McMinnville can prepare the individual, regardless of race, sex, physical or mental abilities, ethnic group, or economic station for employment and/or advancement in the world of work, as well as make a significant contribution to his/her intellectual and social development.

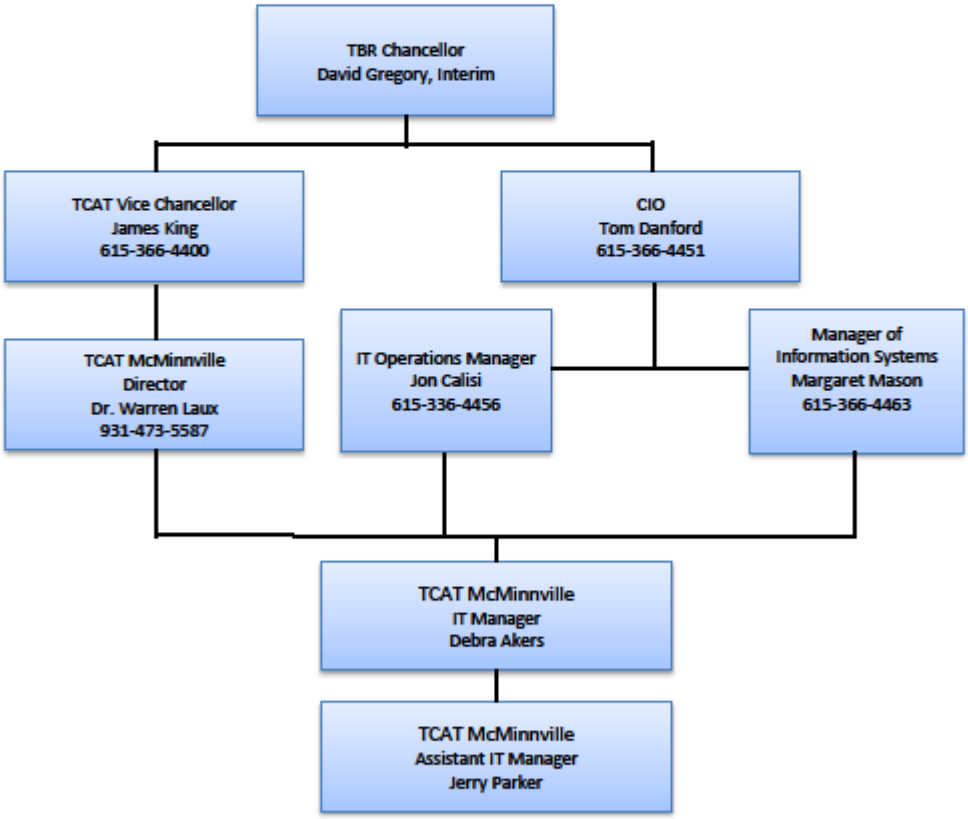
Efforts are made to update equipment and course content to provide educational experience necessary for an era of rapid technological change. The administration and instructional staff are comprised of skilled and knowledgeable personnel who are competent in an occupational field, as well as being proficient instructors.

TCAT McMinnville welcomes and encourages prospective students to visit and see the facilities available. High school students are invited to visit individually, with parents or friends, or in groups scheduled by the high school counselors

Organizational Chart

TENNESSEE COLLEGE OF APPLIED TECHNOLOGY
MCMINNVILLE
241 Vo-Tech Dr. | McMinnville, TN 37110
Phone 931-473-5587 | Fax 931-473-5380

INFORMATION TECHNOLOGY ORGANIZATIONAL CHART



Revised 3/24/2016

IT Personnel

The Tennessee College of Applied Technology - McMinnville's Information Technology Department is responsible for the upkeep and maintenance on the Local Area, Wide Area and Wireless Networks. The IT department will provide technical assistance as needed to the Center.

Information Technology Infrastructure Personnel

IT Manager
Debra Akers
Work: (931) 473-5587 x 245
Cell: (931)607-0186
Reports to Director of TCAT McMinnville
Reports indirectly to IT Department TBR
Coordinates with Office Administrator as needed

Asst. IT Manager
Jerry Parker
Work: (931) 473-5587 x 288
Reports to IT Manager & Director of McMinnville
Reports indirectly to IT Department TBR as needed
Coordinates with Office Administrator as needed

Ethics Policy

Tennessee College of Applied Technology - McMinnville
Information Technology Ethics Policy

1. **Overview**

   Tennessee College of Applied Technology - McMinnville purpose for this ethics policy is to establish a culture of openness, trust and integrity in business practices. Effective ethics is a team effort involving the participation and support of every Tennessee College of Applied Technology - McMinnville employee. All employees should familiarize themselves with the ethics guidelines that follow this introduction.

   Tennessee College of Applied Technology - McMinnville is committed to protecting employees, partners, vendors and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. When Tennessee College of Applied Technology - McMinnville addresses issues proactively and uses correct judgment, it will help set us apart from competitors.

   Tennessee College of Applied Technology - McMinnville will not tolerate any wrongdoing or impropriety at any time. Tennessee College of Applied Technology - McMinnville will take the appropriate measures act quickly in correcting the issue if the ethical code is broken. Any infractions of this code of ethics will not be tolerated.

2. **Purpose**

   Our purpose for authoring a publication on ethics is to emphasize the employees' and consumers' expectation to be treated to fair business practices. This policy will serve to guide business behavior to ensure ethical conduct.

3. **Scope**

   This policy applies to employees, contractors, consultants, temporaries, and other workers at Tennessee College of Applied Technology - McMinnville, including all personnel affiliated with third parties.

4. **Policy**

   4.1. **Executive Commitment to Ethics**

   4.1.1. Management within Tennessee College of Applied Technology - McMinnville must set a prime example. In any business practice, honesty and integrity must be top priority for IT Employees.

4.1.2. IT Employees must have an open door policy and welcome suggestions and concerns from employees. This will allow employees to feel comfortable discussing any issues and will alert IT Employees to concerns within the work force.

4.1.3. IT Employees must disclose any conflict of interests regard their position within Tennessee College of Applied Technology - McMinnville.

4.2. **Employee Commitment to Ethics**

4.2.1. Tennessee College of Applied Technology - McMinnville employees will treat everyone fairly, have mutual respect, promote a team environment and avoid the intent and appearance of unethical or compromising practices.

4.2.2. Every employee needs to apply effort and intelligence in maintaining ethics value.

4.2.3. Employees must disclose any conflict of interests regard their position within Tennessee College of Applied Technology - McMinnville.

4.2.4. Employees will help Tennessee College of Applied Technology - McMinnville to increase customer and vendor satisfaction by providing quality products and timely response to inquiries.

4.3. **Company Awareness**

4.3.1. Promotion of ethical conduct within interpersonal communications of employees will be rewarded.

4.3.2. Tennessee College of Applied Technology - McMinnville will promote a trustworthy and honest atmosphere to reinforce the vision of ethics within the company.

4.4. **Maintaining Ethical Practices**

4.4.1. Tennessee College of Applied Technology - McMinnville will reinforce the importance of the integrity message and the tone will start at the top. Every employee, manager, director needs consistently maintain an ethical stance and support ethical behavior.

4.4.2. Employees at Tennessee College of Applied Technology - McMinnville should encourage open dialogue, get honest feedback and treat everyone fairly, with honesty and objectivity.

4.4.3. Tennessee College of Applied Technology – McMinnville's Director, Assistant Director, and Student Services Coordinator are responsible for making sure the ethical code is delivered to all employees and that concerns regarding the code can be addressed.

4.5. **Unethical Behavior**

4.5.1. Tennessee College of Applied Technology - McMinnville will avoid the intent and appearance of unethical or compromising practice in relationships, actions and communications.

4.5.2. Tennessee College of Applied Technology - McMinnville will not tolerate harassment or discrimination.

4.5.3. Unauthorized use of company trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company will not be tolerated.

4.5.4. Tennessee College of Applied Technology - McMinnville will not permit impropriety at any time and we will act ethically and responsibly in accordance with laws.

4.5.5. Tennessee College of Applied Technology - McMinnville employees will not use corporate assets or business relationships for personal use or gain.

5. Enforcement

5.1.1. Any infractions of this code of ethics will not be tolerated and Tennessee College of Applied Technology - McMinnville will act quickly in correcting the issue if the ethical code is broken.

5.1.2. Any employee found to have violated this policy may be subject to disciplinary action.

Dr. Warren Laux, Director
Marvin Lusk, Assistant Director
Mike Garrison, Student Services Coordinator
Debra Akers, IT Manager
Jerry Parker, Assistant IT Manager

IT Oversight Committee

The IT Department at the Tennessee College of Applied Technology has an oversight committee consisting of the following internal TCAT McMinnville personnel:

Dr. Warren Laux, Director
Marvin Lusk, Assistant Director
Mike Garrison, Student Services Coordinator

The IT Department will meet with the oversight committee once each term. Minutes from the meeting will be on file in the office of the Executive Secretary. Meetings will consist of:

- Policy Review
- Laws and Compliance
- Project Management and Work Orders
- Change Control
- Information Security Program
- ID Theft Program
- BCP (including results of testing)
- IT Risk Assessments
- IT Strategic Planning
- Vendor Management
- Project Management
- Regulatory Oversight (state audit findings)
- Internal Audit Oversight (Audit findings)

Change Control
The procedures for Change Control ensure that all changes are controlled, including the submission, recording, analysis, decision making, and approval of the change.

Recording Changes
In practice, the basic details of a change request from the internally are recorded on a Change Control Request to initiate the change process, including references to documents that describe and authorize the change. This form can be found in the forms directory.

Assessing the Impact, Cost, Benefits, and Risks of Changes
Administration calls a meeting with all persons involved in the change, where the request is to be discussed. All affected groups (e.g., users, management, IT, etc.) are identified and asked to contribute to an assessment of the risk and impact of a

requested change. Through this means, the process is extended well beyond the IT department and draws on input from throughout the school.

Developing the Business Justification and Obtaining Approval
Formal approval should be obtained for each change from the "change authority." The change authority may be a person or a group. The levels of approval for each change should be judged by the size and risk of the change. For example, changes in a large enterprise that affect several distributed groups may need to be approved by a higher-level change authority than a low risk routine change event. In this way, the process is speeded for the routine kinds of changes IT departments deal with every day.

Implementing the Changes
A change should normally be made by a change owner within the group responsible for the components being changed. A release or implementation plan should be provided for all but the simplest of changes and it should document how to back-out or reverse the change should it fail. On completion of the change the results should be reported back for assessment to those responsible for managing changes, and then presented as a completed change for group agreement.

Monitoring and Reporting on the Implementation
The change owner monitors the progress of the change and actual implementation. The people implementing the change update the configuration management database proactively and record or report each milestone of change. Key elements of IT management information can be produced as a result of change management, such as regular reports on the status of changes. Reports should be communicated to all relevant parties.

Closing and Reviewing the Change Requests
The change request and configuration management database should be updated, so that the person who initiated the change is aware of its status. Actual resources used and the costs incurred are recorded as part of the record. A post-implementation review will be done to check that the completed change has met its objectives, that the results are satisfactory; and that there have been no unexpected side-effects. Lessons learned are fed back into future changes as an element of continuous process improvement.

See IT Oversight Committee Folder

Vendor Management

Vendor management enables our school to control costs, drive service excellence and mitigate risks to gain increased value from their vendors throughout the deal life cycle.

TCAT's vendor management is handled by the Coordinator of Fiscal Services who is responsible for selecting the right vendors; categorize vendors to ensure the right contract, metrics and relationship; determine the ideal number of vendors; mitigate risk when using vendors; and establish a vendor management organization that best fits the of our school.

This enables our school to optimally develop, manage and control vendor contracts, relationships and performance for the efficient delivery of contracted products and services. This helps us meet business objectives, minimize potential business disruption, avoid deal and delivery failure, and ensure more-sustainable multi-sourcing, while driving the most value from our vendors.

See Coordinator of Fiscal Services for more information.

Wireless Communication Policy

1.0 Purpose

This policy allows access to Tennessee College of Applied Technology - McMinnville networks via secured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or have been granted an exclusive waiver by The Information Technology Department are approved for connectivity to Tennessee College of Applied Technology - McMinnville's networks.

2.0 Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of Tennessee College of Applied Technology - McMinnville's internal networks. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Tennessee College of Applied Technology - McMinnville's networks do not fall under the purview of this policy.

3.0 Policy

3.1 Register Access Points and Cards

All wireless Access Points / Base Stations connected to the institution network must be registered and approved by The Information Technology Department. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in institution laptop or desktop computers must be registered with The Information Technology Department.

3.2 Approved Technology

All wireless LAN access must use institution-approved vendor products and security configurations.

3.3 VPN Encryption and Authentication

All computers with wireless LAN devices must utilize an institution-approved Internet Access login page configured to block access to any unauthorized device. To comply with this policy, wireless implementations must maintain point to point hardware encryption of at least WPA2. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar. Currently the wireless network supports WPA2 encryption.

3.4 Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

6.0 Revision History
November 30, 2015
March 24, 2016

Patch Management Policy

1.0 Overview
TCAT McMinnville is responsible for ensuring the confidentiality, integrity, and availability of its data and that of customer data stored on its systems. TCAT McMinnville has an obligation to provide appropriate protection against malware threats, such as viruses, Trojans, and worms which could adversely affect the security of the system or its data entrusted on the system. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems within this scope.

2.0 Purpose
This document describes the requirements for maintaining up-to-date operating system security patches on all TCAT McMinnville owned and managed workstations and servers.

3.0 Scope
This policy applies to workstations or servers owned or managed by TCAT McMinnville. This includes systems that contain company or customer data owned or managed by TCAT McMinnville regardless of location. The following systems have been categorized according to management:

- Unix/Lenox servers managed by IT Team
- Microsoft Windows servers managed by IT Team
- Workstations (desktops and laptops) managed by IT Team

4.0 Policy
Workstations and servers owned by TCAT McMinnville must have up-to-date (as defined by GSO's minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by TCAT McMinnville.

4.1 Workstations
Desktops and laptops must have automatic updates enabled for operating system patches. This is the default configuration for all workstations built by TCAT McMinnville.

4.2 Servers
Servers must comply with the minimum baseline requirements. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the TCAT McMinnville asset and the data that resides on the system.

5.0 Roles and Responsibilities

- **IT Team** will manage the patching needs for the Linux servers on the network.
- **IT Team using WSUS Server** will manage the patching needs for the Microsoft Windows servers on the network**.**
- **IT Team using WSUS Server** will manage the patching needs of all workstations on the network.
- **IT Team** is responsible for routinely assessing compliance with the patching policy and will provide guidance to all groups in issues of security and patch management.
- **IT Team using WSUS Server** is responsible for approving the monthly and emergency patch management deployment requests.

6.0 Monitoring and Reporting

Active patching teams noted in the Roles and Responsibility section (5.0) are required monitor the outcome of each patching cycle.

7.0 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of all employees at TCAT McMinnville. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the TCAT McMinnville issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

8.0 Exceptions

Exceptions to the patch management policy require formal documented approval from the IT Team. Any servers or workstations that do not comply with policy must have an approved exception on file with the IT Department.

7.0 Definitions

Term	**Definition**
Patch	A piece of software designed to fix problems with or update a computer program or its supporting data
Trojan	A class of computer threats (malware) that appears to perform a desirable function but in fact performs undisclosed malicious functions
Virus	A computer program that can copy itself and infect a computer without the permission or knowledge of the owner.
Worm	A self-replicating computer program that uses a network to send copies of itself to other nodes. May cause harm by consuming bandwidth.

6.0 Revision History

1.0 initial policy version, 1/27/2016

Security and Monitoring

Debra Akers, IT Manager

Jerry Parker, Asstistant IT Manager

Risk Assessment Policy

1.0 Purpose
To empower IT Department to perform periodic information security risk assessments (RAs) for the purpose of determining areas of vulnerability, and to initiate appropriate remediation.

2.0 Scope
Risk assessments can be conducted on any entity within TCAT McMinnville or any outside entity that has signed a *Third Party Agreement* with TCAT McMinnville. RAs can be conducted on any information system, to include applications, servers, and networks, and any process or procedure by which these systems are administered and/or maintained.

3.0 Policy
The execution, development and implementation of remediation programs is the joint responsibility of IT Department and the department responsible for the systems area being assessed. Employees are expected to cooperate fully with any RA being conducted on systems for which they are held accountable. Employees are further expected to work with the IT Department Risk Assessment Team in the development of a remediation plan.

4.0 Risk Assessment Process
Work In Progress.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms Definitions

Entity - Any business unit, department, group, or third party, internal or external to TCAT McMinnville, responsible for maintaining TCAT McMinnville assets.

Risk - Those factors that could affect confidentiality, availability, and integrity of TCAT McMinnville's key information assets and systems. IT Department is responsible for ensuring the integrity, confidentiality, and availability of critical information and computing assets, while minimizing the impact of security procedures and policies upon business productivity.

7.0 Revision History
November 30, 2015
March 24, 2016

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of TCAT- McMinnville's entire corporate network. As such, all TCAT- McMinnville employees (including contractors and vendors with access to TCAT- McMinnville systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any TCAT- McMinnville facility, has access to the TCAT- McMinnville network, or stores any non-public TCAT- McMinnville information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., root, enable, Admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the IT Department administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at TCAT- McMinnville. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "TCAT- McMinnville", "sanjose", "sanfran" or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters long.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for TCAT- McMinnville accounts as for other non-TCAT-McMinnville access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various TCAT- McMinnville access needs. For example, select one password for the Engineering systems and a separate password for

IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

The student network is an exception to the above rules because it has it's own DSL Line and has no connection at all to the TCAT McMinnville network. The TCAT McMinnville is not trusted by or to the student network. Usernames on the student network corresponds to the computer name which corresponds to each classroom. I.e. if a computer name located in the Computer Lab is Lab-15, then the username is lab15. The password is student for all student access computers.

Do not share TCAT- McMinnville passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential TCAT-McMinnville information.

Here is a list of "dont's":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to IT Department and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT Department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards
Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
- should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users
Access to the TCAT- McMinnville Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases
Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions
Terms Definitions
Application Administration Account - Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History
11/30/2015

Virtual Private Network (VPN) Policy

Currently no VPNs are allowed to provide access to the TCAT McMinnville networks. In the event that any VPN is to be established at a future date the following guidelines will apply:

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the TCAT - McMinnville institution network.

2.0 Scope
This policy applies to all TCAT - McMinnville employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the TCAT - McMinnville network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator.

3.0 Policy
Approved TCAT - McMinnville employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the *Remote Access Policy*.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to TCAT - McMinnville internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the institution network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by TCAT - McMinnville network operational groups.
6. All computers connected to TCAT - McMinnville internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the institution standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from TCAT - McMinnville's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not TCAT - McMinnville-owned equipment must configure the equipment to comply with TCAT - McMinnville's VPN and Network policies.
10. Only IT Department-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of TCAT - McMinnville's network, and as such are subject to the same rules and regulations that apply to TCAT - McMinnville-owned equipment, i.e., their machines must be configured to comply with IT Department's Security Policies.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Term Definition

IPSec Concentrator - A device in which VPN connections are terminated.

6.0 Revision History

November 30, 2015

Disaster Recovery and Backup

The following servers are backed up to the Carbonite Cloud after being backed up locally to NAS:

TTCM-STUDENTDAT

*Student Data Files (Non mission essential)
*Solid Works licensing (Mission Critical) - Requires Dongle
*IEE Movies (Mission Critical)
*MTT Projects (Mission Critical)

TTCM-STAFFDATA

*School Software (Mission Critical)
*All instructor / staff folders (Mission Critical)
*Accounting (Mission Critical)
*Office Movies (Mission Critical)
*All instructor / staff folders (Mission Critical)

SIMSERVER

*SIM (Mission Critical)
*SQL Server 2005 SIM Database/DPC Database/TomCat
(This information is also stored offsite in Paris Tennessee – Encrypted)

Firewall Server

*Logs
*DIY74 (Bell) (Mission Critical)
*Emergency SMS numbers (Cell Numbers)

All backups are backed up to an internal drive and/or NAS.
Critical files are backed up to the Carbonite Cloud Backup System

Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to TCAT-McMinnville's network from any host. These standards are designed to minimize the potential exposure to TCAT-McMinnville from damages which may result from unauthorized use of TCAT-McMinnville resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical TCAT-McMinnville internal systems, etc.

2.0 Scope

This policy applies to all TCAT-McMinnville employees, contractors, vendors and agents with a TCAT-McMinnville-owned or personally-owned computer or workstation used to connect to the TCAT-McMinnville network. This policy applies to remote access connections used to do work on behalf of TCAT-McMinnville, including reading or sending email and viewing intranet web resources.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of TCAT-McMinnville employees, contractors, vendors and agents with remote access privileges to TCAT-McMinnville's institution network to ensure that their remote access connection is given the same consideration as the user's on-site connection to TCAT-McMinnville.
2. General access to the Internet for recreational use by immediate household members through the TCAT-McMinnville Network on personal computers is permitted for employees that have flat-rate services. The TCAT-McMinnville employee is responsible to ensure the family member does not violate any TCAT-McMinnville policies, does not perform illegal activities, and does not use the access for outside business interests. The TCAT-McMinnville employee bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the institution network via remote access methods, and acceptable use of TCAT-McMinnville's network:
    a. *Acceptable Encryption Policy*
    b. *Virtual Private Network (VPN) Policy*
    c. *Wireless Communications Policy*
    d. *Acceptable Use Policy*

4. For additional information regarding TCAT-McMinnville's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., go to the Remote Access Services website.

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases. For information on creating a strong pass-phrase see the Password Policy.
2. At no time should any TCAT-McMinnville employee provide their login or email password to anyone, not even family members.
3. TCAT-McMinnville employees and contractors with remote access privileges must ensure that their TCAT-McMinnville-owned or personal computer or workstation, which is remotely connected to TCAT-McMinnville's institution network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
4. TCAT-McMinnville employees and contractors with remote access privileges to TCAT-McMinnville's institution network must not use non-TCAT-McMinnville email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct TCAT-McMinnville business, thereby ensuring that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the TCAT-McMinnville network must meet minimum authentication requirements of CHAP.
6. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and IT Department must approve security configurations for access to hardware.
9. All hosts that are connected to TCAT-McMinnville internal networks via remote access technologies must use the most up-to-date anti-virus software, this includes personal computers. Third party connections must comply with requirements as stated in the *Third Party Agreement*.
10. Personal equipment that is used to connect to TCAT-McMinnville's networks must meet the requirements of TCAT-McMinnville-owned equipment for remote access.
11. Organizations or individuals who wish to implement non-standard Remote Access solutions to the TCAT-McMinnville production network must obtain prior approval from Remote Access Services and IT Department.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Term Definition
Cable Modem - Cable companies such as AT&T Broadband provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps. Cable is currently available only in certain communities.

CHAP - Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function. DLCIData Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network, and has local significance only to that channel.

Dial-in Modem - A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

Dual Homing - Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the Institution network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a TCAT-McMinnville-provided Remote Access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into TCAT-McMinnville and an ISP, depending on packet destination.

DSL - Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Frame Relay - A method of communication that incrementally can go from the speed of an ISDN to the speed of a T1 line. Frame Relay has a flat-rate billing charge instead of a per time usage. Frame Relay connects via the telephone company's network.

ISDN - There are two flavors of Integrated Services Digital Network or ISDN: BRI and PRI. BRI is used for home office/remote access. BRI has two "Bearer" channels at 64kbit (aggregate 128kb) and 1 D channel for signaling info.

Remote Access - Any access to TCAT-McMinnville's institution network through a non-TCAT-McMinnville controlled network, device, or medium.

Split-tunneling - Simultaneous direct access to a non-TCAT-McMinnville network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into TCAT-McMinnville's institution network via a VPN tunnel. VPN Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet.

6.0 Revision History
November 30, 2015

Server Security Policy

1.0 Purpose
The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by TCAT McMinnville. Effective implementation of this policy will minimize unauthorized access to TCAT McMinnville proprietary information and technology.

2.0 Scope
This policy applies to server equipment owned and/or operated by TCAT McMinnville, and to servers registered under any TCAT McMinnville-owned internal network domain.

This policy is specifically for equipment on the internal TCAT McMinnville network. For secure configuration of equipment external to TCAT McMinnville on the DMZ, refer to the *Internet DMZ Equipment Policy*.

3.0 Policy

3.1 Ownership and Responsibilities
All internal servers deployed at TCAT McMinnville must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by The Information Technology Department. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group must establish a process for changing the configuration guides, which includes review and approval by The Information Technology Department.

- Servers must be registered within the institution enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the institution enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures.

3.2 General Configuration Guidelines
- Operating System configuration should be in accordance with approved The Information Technology Department guidelines.

- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental tape backups will be retained for at least 1 month.
    - Weekly full tape backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to The Information Technology Department, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

3.4 Compliance

- Audits will be performed on a regular basis by authorized organizations within TCAT McMinnville.
- Audits will be managed by the internal audit group or The Information Technology Department, in accordance with the *Audit Policy*. The Information Technology Department will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation or justification.

- Every effort will be made to prevent audits from causing operational failures or disruptions.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Term Definition
DMZ - De-militarized Zone. A network segment external to the institution production network.

Server - For purposes of this policy, a Server is defined as an internal TCAT McMinnville Server. Desktop machines and Lab equipment are not relevant to the scope of this policy.

6.0 Revision History
November 30, 2015

Guidelines on Anti-Virus Process

Recommended processes to prevent virus problems:

- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with TCAT McMinnville's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a USB drives from an unknown source for viruses before using it.
- Back-up critical data and system configurations on a regular basis and store the data in a safe place.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

Revision History
1/1/2015
11/30/2015

Workstation Security Policy

1.0 Purpose
The purpose of this policy is to provide guidance for workstation security for TCAT-MCMINNVILLE workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

2.0 Scope
This policy applies to all TCAT-MCMINNVILLE employees, contractors, workforce members, vendors and agents with a TCAT-MCMINNVILLE - owned or personal-workstation connected to the TCAT-MCMINNVILLE network.

3.0 Policy
Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitivity information, including protected health information (PHI) and that access to sensitivity information is restricted to authorized users. Laptops will in addition be logged out on a computer log located in the CIT Department.

3.1 Workforce members using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and minimize the possibility of unauthorized access.

3.2 TCAT-MCMINNVILLE will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

3.3 Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.

- Never installing unauthorized software on workstations. (All software installations must be approved by IT Team.
- Storing all sensitivity information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitivity information by using cable locks or locking laptops up in drawers or cabinets.
- Complying with the Portable Workstation Encryption policy
- Complying with the Anti-Virus policy
- Ensuring that monitors are positioned away from public view. If necessary, install privacy screen filters or other physical barriers to public viewing.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates. Exit running applications and close open documents.
- Ensuring that all workstations use a surge protector (not just a power strip) or a UPS (battery backup).
- If wireless network access is used, ensure access is secure by following the Wireless Access policy

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Workstations include: laptops, desktops, MOBILE DEVICESs, computer based medical equipment containing or accessing patient information and authorized home workstations accessing the TCAT-MCMINNVILLE network.

Workforce members include: employees, volunteers, trainees, and other persons under the direct control of TCAT MCMINNVILLE.

6.0 Revision History
11/30/2015

Acceptable Encryption Policy

1.0 Purpose
The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and legal authority is granted for the dissemination and use of encryption technologies outside of the United States.

2.0 Scope
This policy applies to all Tennessee College of Applied Technology - McMinnville employees and affiliates.

3.0 Policy
Proven, standard algorithms such as DES, Blowfish, RSA, RC5 and IDEA should be used as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hellman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Tennessee College of Applied Technology - McMinnville's key length requirements will be reviewed annually and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by InfoSec. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions
Term Definition
Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

Symmetric Cryptosystem - A method of encryption in which the same key is used for both encryption and decryption of the data.

Asymmetric Cryptosystem - A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (e.g., public-key encryption).

Website Management

TCAT McMinnville's website address is www.tcatmcminnville.edu. The initial website was set up by TBR based on the same general theme and look for all TCATs across the state. The responsibility of maintaining and updating the site is that of Debra Akers at the TCAT McMinnville.

In addition to publishing information on the website, the public is able to complete and submit applications for enrollment from the site. This data is automatically send via email to the appropriate staff for processing.

TBR's Web Publishing Policy: SO-Chan-Web are followed when publishing any information to the website. Below is the policy:

Purpose

The Tennessee Board of Regents (TBR) websites exist as the Board's most important communication tool. Therefore, websites should maintain and build upon the projected image of TBR through the highest level of excellence in education, policy, research, and workforce development by concerning the administration with the digital image projected. This policy should facilitate usability and consistency and promote a cohesive online brand throughout all TBR websites that correlates directly with other TBR methods of communication and visual representation.

Policy/Guideline

1. Goals
    1. Identify a consistent brand for the TBR system and all of its programs and services.
    2. Effectively serve students, faculty, staff, legislators, and other people of interest with useful and easily accessible information.
    3. Provide easy to use information and services on as many devices as possible.
    4. Promote a positive impression of TBR, its staff, and its institutions with a unified and compelling image.
    5. Promote ease of use with intuitive web standards.
    6. Present TBR and its activities as a seamless entity.
2. Scope
    1. Any Web document that represents the TBR, its units and their activities, its initiatives, its programs and collaborations, and its contractors and partners, while having its own purpose and agenda, is also part of the whole and, therefore, needs to be clearly identified with the TBR brand

and is expected to follow this policy. This policy does not apply to member institutions.

3. Manager
    1. Within the Chancellor's Office, the Web Systems & Digital Media Manager (hereafter 'web manager') maintains and enforces this policy, including any granted exceptions, and has primary responsibility for the content, format and appearance of all web pages and systems.
    2. Under the direction of the Chief Information Officer and guidance from the web manager, the Office of Information Technology will maintain the TBR web infrastructure.
4. Content Managers
    1. Content managers must be classified as permanent TBR staff or an approved third-party vendor who works under the direct supervision of the web manager.
    2. Request for access must be submitted for each unit. The web manager and the unit's leader must approve each access request.
    3. Management of web content, including web pages, media and data, and ensuring that pages within their unit are up to date, meaningful and appropriate, and follow the official TBR Electronic Publishing and Web Style Guide, is the sole responsibility of the corresponding department and their designated content manager(s).
    4. Web content ownership and responsibility will be directed to the Vice Chancellors who are ultimately responsible for all units and their activities.
5. Guidelines
    1. Use
        1. TBR websites may only be used for official board, administrative and educational activities.
        2. Websites must comply with all IT policies regarding the use of TBR resources.
    2. Organization
        1. All websites should strive to be a part of the overall web structure of the TBR. No unit may go outside the TBR web structure and represent itself or activities unless an exception is granted by the web manager.
        2. The TBR web structure is as follows:
            1. Administrative Offices, Policies, & the Board
            2. Community College System
            3. University System
            4. Colleges of Applied Technology System
            5. Regents Online Campus Collaborative
            6. Internal Use Applications
    3. Web Projects

1. All website projects must be submitted in writing to the web manager for a feasibility evaluation.
2. All websites, when feasible, should be developed in-house and within the available systems.
3. If the web manager determines a project cannot be completed in-house, the web manager must serve on the selection committee and as project manager or co-project manager with the contracted agency and has final approval before a project is launched.
4. All websites associated with the TBR and its affiliate groups must follow the current approved TBR web template maintained by the web manager

4. Layout and Design Elements
    1. All TBR websites should follow the official TBR Electronic Publishing and Web Style Guide.
    2. When possible, all sites should be developed device agnostic.
    3. Visible credits such as "Site powered by..." or "Site created by..." are prohibited.
    4. Federal law and guidance letters regarding nondiscrimination policies require that the nondiscrimination statement be available. The official statement will be provided in the Electronic Publishing and Web Style Guide.
5. Accessibility
    1. All TBR websites are subject to the same accessible web standards as state and federal agencies. Section 508 of the Federal Register establishes requirements for federal electronic and information technology, and the federal Access Board has issued the standards to meet those requirements.
    2. Websites should be accessible for those using assistive methods and/or alternative methods to access the Web.
    3. All TBR websites should have a link to the TBR's top-level "Web Accessibility" page.
6. Domains and Subdomains
    1. All domains and related product purchases (secure certificates, etc.) must be made through the Office of Information Technology.
    2. The approved domain names for all TBR web systems are:
        1. tbr.edu;
        2. rodp.org.
    3. The web manager may make an exception for promotional URLs or collaboratives with other systems/partners, (eg. tntransferpathways.org). Unless noted in the exception, all promotional domains must forward to a TBR.edu page or subdomain.
7. Content Validity

1. Content must be kept up-to-date and relevant.
2. Any website or page deemed as outdated or incorrect may be changed or removed by the web manager.

8. Disclaimer of Endoresements
    1. The TBR does not endorse or recommend any commercial products, processes, or services. Therefore, mention of commercial products, processes, or services on TBR websites must be written in a way as they may not be construed as an endorsement or recommendation.
    2. When users select a link to an external website, users must be made aware they are subject to the privacy and security policies of the owners/sponsors of the external site. Official language will be provided in the Electronic Publishing and Web Style Guide.
9. Redundancy
    1. Redundant information, especially different published versions of content, can be confusing and may result in severe consequences if incorrect or outdated information is posted. Only publish the latest version of content.
    2. Repeating static information maintained elsewhere should not be copied but rather linked or be displayed by the use of a data feed such as RSS, XML, or database API.
10. Copyright
    1. All material used on TBR websites must comply with federal and state copyright laws, including respecting proper licensing rights for purchased reports, data, images, video, and text.
11. Exceptions and Exemptions
    1. The web manager may exempt certain web applications that are technically limited in their ability to meet the necessary guidelines from those guidelines.
    2. Exemptions noted in this document should be requested in writing to the web manager.

Tennessee Board of Regents Privacy Statement for websites

The privacy, confidence, and trust of individuals who visit Tennessee Board of Regents (TBR) web sites are important to us. No personal information is collected at this site unless it is provided voluntarily by an individual while participating in an activity that asks for the information. The following paragraphs disclose the information gathering and usage practices for the web site.

Collection of Information

The TBR only collects the personally identifiable information that is necessary to provide the information or services requested by an individual [LPS1]. "Personal information"

refers to any information relating to an identified or identifiable individual. This is the same information that an individual might provide when visiting a government office and includes such items as an individual's name, address, or phone number. The TBR uses the collected information to respond appropriately to requests. This may be to respond directly to you or to improve the web site. E-mail or other information requests sent to the TBR web site may be maintained or forwarded to the appropriate agencies in order to respond to the request. Survey [LPS2] information is used for the purpose designated in the survey.

The TBR also collects statistical information that helps us understand how people are using the web site so we can continually improve our services. The information collected is not associated with any specific individual [LPS3] and no attempt is made to profile individuals who browse the web site. This information includes, but is not limited to:

- Device-specific information (hardware, operating system, language and browser type)
- Log information (IP address, search queries and referral URL)
- Local storage, cookies[LPS4] and anonymous identifiers to collect and store information locally on your device

Web Site Security

The TBR is committed to the security of the information that is either available from or collected by this web site. The TBR has taken multiple steps to safeguard the integrity of its telecommunications and computing infrastructure, including but not limited to, authentication, monitoring, auditing, encryption (SSL) and various physical safeguards.

Links to Other Sites

This web site has links to many other web sites. These include links to web sites operated by other government agencies, nonprofit organizations, and private businesses. The TBR is not responsible for the content or privacy practices of these sites and suggests you review their privacy statements.

FERPA Rights to Privacy

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.

FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

For more information on FERPA, please see the Department of Education web site.

Application

Our Privacy Statement applies to all web sites and services offered by the TBR, its units and their activities, its initiatives, its programs and collaborations, and work being done on behalf of the TBR by its contractors and partners, but exclude services that have separate privacy statements. The TBR Privacy Statement does not apply to its member institutions.

Changes

The TBR Privacy Statement may be changed at any time without notice or consent. All changes will be posted on the web site.

DATA PROCESSING OPERATIONS

All data generated or processed is per the individual department guidelines. Secure servers located in the server room are used for internal data storage. The internal network is not accessible by VPN, and is separate and apart from the student and wireless networks. All data is backed up daily on local backup server. Student database is additionally backed up by DPC on their servers located in Memphis, TN.

Non-sensitive data may be exported or transmitted by encrypted email. Sensitive data is transmitted by sftp to secure servers located either on the main Motlow Campus in Tullahoma, TN or TBR Servers located in Nashville, TN.

Sensitive data is only to be stored on jump drives that are encrypted.

Retention of Information

Records needed to support TBR program functions are retained, managed, and accessible in record keeping or filing systems in accordance with established records disposition authorizations approved by the State of Tennessee's Public Records Commission. Records transmitted to this site will be identified, managed, protected, and retained as long as they are needed to meet historical, administrative, fiscal, or legal requirements.

Public Disclosure

Regardless of whether information is provided to the TBR by personal visit, mail, or web site, it becomes public record and is open to public inspection unless protected by State or Federal law. Public records are subject to the rules and requirements located in Tennessee Code Annotated Title 10 Chapter 7. A public record is defined as follows:

> "Public record(s)" or "state record(s)" 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. (T.C.A. 10-7-301 (6))

Based on the definition of public records, be aware that any information collected at this site could be made available to the public. Requests for public records will be examined for compliance with public record laws.

Identity Theft Prevention Policy

(Based on TBR Identity Theft Prevention: 4:01:05:60

Purpose

The Tennessee Board of Regents, on behalf of its Institutions, 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
    1. The risk to the institutions of the Tennessee Board of Regents (hereinafter referred to as "Institutions"), 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.

2. Under this Policy the program will:
    1. 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);
    2. Detect red flags that are incorporated in the program;
    3. Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft;
    4. 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,
    5. Promote compliance with state and federal laws and regulations regarding identity theft protection.
3. 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
    1. 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.
    2. Alerts, notifications or warnings from a credit or consumer reporting agency. Examples of these red flags include the following:
        1. A report of fraud or active duty alert in a credit or consumer report;
        2. A notice of credit freeze from a credit or consumer reporting agency in response to a request for a credit or consumer report;
        3. A notice of address discrepancy in response to a credit or consumer report request; and,
        4. 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.

3. Suspicious documents. Examples of these red flags include the following:
    1. Documents provided for identification that appears to have been altered, forged or are inauthentic.
    2. The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
    3. Other information on the identification is not consistent with information provided by the person opening a new covered account or individual presenting the identification.
    4. 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.
    5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
4. Suspicious personal identifying information. Examples of these red flags include the following:
    1. 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.
    2. 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.
    3. 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.
    4. 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.

5. The social security number provided is the same as that submitted by another person opening an account.
6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by that of another person.
7. 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.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the Institution.
9. 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.

5. Unusual use of, or suspicious activity related to, the covered account. Examples of these red flags include the following:
    1. 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.
    2. 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.
    3. 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).
    4. Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
    5. The Institution is notified that the individual is not receiving paper account statements.
    6. The Institution is notified of unauthorized charges or transactions in connection with an individual's covered account.
    7. 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.
    8. 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.

9. A breach in the Institution's computer security system.

3. Detecting Red Flags
    1. 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:
        1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and,
        2. 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.
    2. 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:
        1. Verify the identification of students if they request Information;
        2. 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,
        3. Verify changes in banking information given for billing and payment purposes.
    3. 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:
        1. 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
        2. 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
    1. 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.
    2. The Institution should quickly gather all related documentation, write a description of the situation and present this information to the Program Administrator for determination.
    3. The Program Administrator (see Section VI) will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
    4. The Institution may take the following steps as is deemed appropriate:

1. Continue to monitor the covered account for evidence of identity theft;
2. Contact the student or applicant for which a credit report was run;
3. Change any passwords or other security devices that permit access to covered accounts;
4. Close and reopen the account;
5. Determine not to open a new covered account;
6. Provide the student with a new student identification number;
7. Notify law enforcement;
8. Determine that no response is warranted under the particular circumstances;
9. Cancel the transaction.

5. Protecting Personal Information
    1. 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:
        1. Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
        2. Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
        3. 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.
        4. 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.
        5. Ensure that office computers with access to covered account information are password protected.
        6. Ensure that computer virus protection is up to date.
        7. Avoid the use of social security numbers.
        8. Utilize encryption devices when transmitting covered account information.
    2. Institutional personnel are encouraged to use common sense judgment in securing covered account information to the proper extent.
    3. 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.

4. 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
    1. Oversight and Appointment of the Institutional Program Administrator
        1. 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.
        2. 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.
        3. 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.
        4. 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.
        5. A report to the Institution's President or 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.
    2. Staff training
        1. 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.

3. Periodic Updates to the Program
    1. 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.
    2. 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.
    3. 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.
    4. Actions to take in the event that fraudulent activity is suspected or discovered may also require revision to the program.
4. Overview of service provider arrangements
    1. 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.
    2. 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.
            1. Specific language for inclusion in contracts can be found in TBR Guideline G-030 Contracts and Agreements.
    3. 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.

Sources

March 26, 2009 Board meeting; June 19, 2009.

Information Technology and Infrastructure Summary

(**Laws-Compliance**)

Debra Akers, IT Manager

Jerry Parker, Assistant IT Manager

Internet Responsible Use Policy

Accessing Inappropriate Materials - Accessing, submitting, posting, publishing, forwarding, downloading, scanning or displaying materials that are defamatory, abusive, obscene, vulgar, sexually explicit, sexually suggestive, threatening, discriminatory, harassing and/or illegal;

Illegal Activities - Using the institution unit's computers, networks and Internet services for any illegal activity or activity that violates other board policies, procedures and/or institution rules;

Violating Copyrights - Copying or downloading copyrighted materials without the owner's permission;

Plagiarism - Representing as one's own work any materials obtained on the Internet (such as term papers, articles, etc.). When Internet sources are used in student work, the author, publisher and Web site must be identified;

Copying Software - Copying or downloading software without the express authorization of the system administrator;

Non-Institution-Related Uses - Using the institution unit's computers, networks and Internet services for non-institution-related purposes such as private financial gain, commercial, advertising or solicitation purposes, or for any other personal use;

Misuse of Passwords/Unauthorized Access - Sharing passwords, using other users' passwords without permission and/or accessing other users' accounts;

Malicious Use/Vandalism - Any malicious use, disruption, or harm to the institution unit's computers, networks and Internet services, including but not limited to hacking activities and creation/uploading of computer viruses; and

Unauthorized Access to Chat Rooms/News Groups - Accessing chat rooms or news groups without specific authorization from the supervising teacher.

The institution IT Dept. retains control, custody and supervision of all computers, networks and Internet services owned or leased by the institution unit. The institution IT Dept. reserves the right to monitor all computer and Internet activity by students. Students have no expectation of privacy in their use of institution computers, including e-mail and stored files.

Responsible Use Policy

Based on RUP of the Tennessee Board of Regents (Appendix B, page 99)

TABLE OF CONTENTS

1. Introduction

This document constitutes the policy for the management of all computers, computer-based networks and all related equipment made available by the TCAT-McMinnville. The policy reflects the ethical principles of the TCAT McMinnville community and indicates, in general, the privileges and responsibilities of those using TCAT McMinnville computing and networking resources. Because some networks operate in environments in which specific items in this policy do not apply, system administrators are permitted, with prior approval of the *Information Technology Committee*, to create written policies that are at variance with this one, as long as the principles related to legal use and institutional purposes are preserved. In such cases, it is the responsibility of system administrators to make relevant variances known to their users.

This document informs all users of the policies set forth by TCAT McMinnville, in compliance with the Tennessee Board of Regents, the State of Tennessee, and the Federal government

2. Existing TCAT McMinnville Policies and Regulations

This policy is intended to be an addition to existing TCAT McMinnville policies and regulations, and does not alter or modify any existing TCAT McMinnville policy or regulation.

3. Definitions

The following terms shall have the following meanings when used in this document:

Administrator - The person having executive authority over one or more computing resources.

Central Computing Resource - Computers and peripherals purchased, maintained, and operated by the Computer Operations Technology Information Technology Department and made available to the TCAT McMinnville community.

Communications System Center - Any TCAT McMinnville voice, video, or data network and the components of such networks.

Computer Account - Computer account codes (called userID's) that provide access to computer networks are made available to faculty, retired faculty, staff and registered students to assist them in carrying out the instructional, research, and administrative goals of the TCAT McMinnville. Other persons may qualify for public service or guest accounts on a particular system with approval of the administrator and such use does not exceed 5% of resources used on that system.

Data Owner - The individual or unit that can authorize access to information, data, or software and that is responsible for the integrity and accuracy of that information, data, or software.

Departmental Computing Resource - Computers and peripherals purchased by an institutional unit primarily for the use of personnel within that entity.

Individual Computing Resource - All computers and peripherals purchased by the institutional , primarily for the use of an individual member of that unit and computers personally owned by faculty, staff or students which use TCAT McMinnville resources on-campus and/or off-campus.

Networked Computing Resource - All computers and peripherals connected to any TCAT McMinnville network.

Shared Computing Resource - Computers and associated peripherals that are commonly used, simultaneously, by more than one person.

System Administrator - The person or group who has system privileges and is responsible for the operation and security of one or more networked computing resources.

Unit - The individual, group or organization responsible for performing a function within the TCAT McMinnville community.

User - Any individual who has access to a computing and computer-based network resource.

4. Ethical Behavior and Rights

The TCAT McMinnville, by its very nature, values openness and promotes access to a wide range of information. Campus information systems have been designed to be as open as possible, and as such, the TCAT McMinnville insists on responsible use of these systems. The use of computers, computer-based networks, and electronic information is essential for research, instruction and administration within the academic community. Because the electronic environment is easily disrupted and electronic information is readily reproduced, respect for the work and rights of others is especially important.

Any intentional behavior with respect to the electronic environment that interferes with the mission or activities of the TCAT McMinnville or members of the TCAT McMinnville community will be regarded as unethical and may lead to disciplinary action under standard TCAT McMinnville rules.

Users have the right to free inquiry and expression consonant with the purposes of the TCAT McMinnville. Users have the right to keep certain data reasonably confidential, such as electronic mail correspondence and data files. However, they must recognize that data storage and communications are not perfectly secure. There are software and physical limitations that can compromise security.

5. Copyrights

Software available on computers and networks is not to be copied except as permitted by the applicable software license. The TCAT McMinnville is a member of Tennessee Board of Regents (TBR), and adheres to the Code of Software and Intellectual Rights:

> "Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principal applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.
>
> Because electronic information is volatile and easily reproduces, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community."

Quoted from: Using Software: A Guide to the Ethical and Legal Use of Software for Members of the Academic Community, TBR (EDUCOM January 1992), p.3.

6. General Responsibilities

Any individual using the TCAT McMinnville's computing and/or computer-based network resources or facilities has the following responsibilities:

To use the TCAT McMinnville's computing facilities and information resources, including hardware, software, networks and computer accounts, responsibly and appropriately, respecting the rights of other computing users and respecting all contractual and license agreements.

To use only those computers and computer accounts for which authorization has been given to that person.

To be responsible for all use of accounts and for protecting each account's password. The sharing of accounts is not permitted. If someone else learns an individual's password, it must be changed.

To report unauthorized use of any accounts to the project director, instructor, supervisor, system administrator or other appropriate TCAT McMinnville authority.

To take reasonable and appropriate steps to see that all hardware and software license agreements are faithfully executed on any system, network or server that is used.

Do not misuse computing, computer-based networks and/or information resources and privileges associated with their use should not be misused by any of the following:

- Attempting to modify or remove computer equipment, software, or peripherals without proper authorization.
- Accessing computers, computer software, computer data or information, or networks without proper authorization, regardless of whether the computer, software, data, information, or network in question is owned by the TCAT McMinnville (That is, if you abuse the networks to which the TCAT McMinnville belongs or the computers at other sites connected to those networks, the TCAT McMinnville will treat this matter as an abuse of your TCAT McMinnville computing privileges.)
- Circumventing or attempting to circumvent normal resource limits, logon procedures, and security regulations.
- Using computing facilities, computer accounts, or computer data for purposes other than those for which they were intended or authorized.
- Ending any fraudulent electronic transmission, including but not limited to fraudulent requests for confidential information.

- Violating any software license agreement or copyright, including copying or redistributing copyrighted computer software, data, or reports without proper, recorded authorization.
- Violating the property rights of copyright holders who are in possession of computer-generated data, reports, or software.
- Using the TCAT McMinnville's computing resources to harass or threaten other individuals.
- Taking advantage of another user's naiveté or negligence to gain access to any computer account, data, software, or file which has not had explicit authorization has been given.
- Physically interfering with other users' access to the TCAT McMinnville's computing facilities.
- Encroaching on others' use of the TCAT McMinnville's computers (e.g., disrupting others' computer use by excessive game playing; by sending excessive messages, either locally or off-campus [including but not limited to electronic chain letters]; printing excessive copies of documents, files, data, or programs; modifying system facilities, operating systems, or disk partitions; attempting to crash or tie up a TCAT McMinnville computer; damaging or vandalizing TCAT McMinnville computing facilities, equipment, software, or computer files).
- Disclosing or removing proprietary information, software, printed output or magnetic media without the explicit permission of the owner.
- Reading other users' data, information, files, or programs on a display screen, as printed output, or via electronic means, without the owner's explicit permission.
- Posting or sending obscene, pornographic, sexually explicit, or offensive material.
- Posting or sending material that is contrary to the mission or values of the TCAT McMinnville.
- Intentional or negligent distribution of computer viruses.
- Using computing and computer-based networks for commercial purposes.

7. External Networks

Members of the TCAT McMinnville community who use networks, facilities, or computers not owned by the TCAT McMinnville shall adhere to this policy and all policies and procedures established by the administrators of non-TCAT McMinnville networks, facilities, or computers they use (policies and procedures can usually be obtained from the network information center of the network in question). Whether or not an external policy exists, the TCAT McMinnville Policy shall remain in effect and shall be adhered to by members of the TCAT McMinnville community at all times.

8. Privacy Considerations

In an operational sense, files in personal accounts and data on the network are regarded as private: that is, employees of the TCAT McMinnville do not routinely look at this information. However, the TCAT McMinnville reserves the right to view or scan any file or software stored on TCAT McMinnville systems or transmitted over TCAT McMinnville networks, and may do so periodically to verify that software and hardware are working correctly, to look for particular kinds of data or software (such as computer viruses), or to audit the use of TCAT McMinnville resources. Violations of policy that come to the TCAT McMinnville's attention during these and other activities will be acted upon.

Individual data on TCAT McMinnville computing systems may be copied to backup tapes periodically. The TCAT McMinnville makes reasonable efforts to maintain confidentiality, but if an individual wishes to ensure confidentiality, that person is advised to encrypt the data in question. Although use of encryption software is permitted, individuals are responsible for remembering encryption keys. Once the data is encrypted, the TCAT McMinnville will be unable to help recover it if the encryption key is forgotten or lost.

When sources outside the TCAT McMinnville request an inspection and/or examination of any TCAT McMinnville owned or operated communications system, computing resource, and/or files or information contained therein, the TCAT McMinnville will treat information as confidential unless any one or more of the following conditions exist:

Approved by the appropriate TCAT McMinnville official(s) or the head of the Department to which the request is directed

Authorized by the owner(s) of the information

Required by federal, state, or local law

Required by a valid subpoena or court order

Note: When notice is required by law, court order, or subpoena, computer users will receive prior notice of such disclosures (viewing information in the course of normal system maintenance does not constitute disclosure).

9. Electronic Mail (e-mail)

E-mail is privileged communication between the parties involved and should be subject to all of the same protections afforded to traditional "paper" mail. When a user sends e-mails, the user account identification is included in each mail message. The user is responsible for all e-mail originating from the user's account. Therefore:

Forgery or attempted forgery of e-mail messages is prohibited.

Attempts to read, delete, copy, or modify the e-mail of other users are prohibited. Sending or attempts to send harassing, obscene and/or other threatening e-mail to another user is prohibited.

Sending or attempts to send unsolicited junk mail, "for-profit" messages or chain letters is prohibited.

Flooding or attempts to flood a user's mailbox is prohibited.

Employees should be aware that electronic mail and messages sent through computer networks, including the Internet, may not remain confidential while in transit or on the destination computer system.

10. World Wide Web Home Pages

In order to encourage mutual sharing of information, creativity, diversity, and technical knowledge within the campus community and beyond, the TCAT McMinnville offers to authorized users of computing resources the use of its facilities for publishing information on the World Wide Web. Certain restrictions as to platforms available for WWW publishing and resources allotted may be necessary due to system limitations.

Individual WWW pages may contain information on the research and other activities and interests of individuals, samples of original creative work, along with links to other sources of information on these topics. Student home pages may serve as resumes or portfolios that may be viewed by prospective employers.

Publishers of Web pages must avoid the use of inflammatory or offensive language and symbols in their individual home pages. Due to the public nature of Web publishing, and the increasing number of K-12 students who are accessing it, individual home pages must not contain violent or prurient material, or provide links to sites which contain such material.

Because individual home pages are the intellectual property of the individual, publishers of home pages must refrain from representing their pages as an official TCAT McMinnville publication. Use of TCAT McMinnville insignia or logos is specifically prohibited.

Individual home pages are subject to all applicable provisions contained in this Policy and/or other applicable institutional policies.

The TCAT McMinnville may provide resources for WWW pages, but it takes no responsibility for the individual opinions expressed therein. However, it reserves the

right to monitor content and to terminate access to any pages which are not in compliance with this policy.

11. Sanctions

Violations of this Policy shall subject users to the regular disciplinary processes and procedures of the TCAT McMinnville for students, staff, administrators, and faculty, and may result in loss of their computing privileges.

Illegal acts involving TCAT McMinnville computing resources may also subject violators to prosecution by local, state, and/or federal authorities.

12. Disclaimer

As part of the services available through the TCAT McMinnville's campus network, access is provided to a large number of conferences, lists, bulletin boards, and Internet information sources. These materials are not affiliated with, endorsed by, edited by, or reviewed by the TCAT McMinnville, and the TCAT McMinnville takes no responsibility for the truth or accuracy of the content found within these information sources. Moreover, some of these sources may contain material that is offensive or objectionable to some users.

Email Policies

Email Retention Policy

1.0 Purpose
The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to IT Department.

2.0 Scope
This email retention policy is secondary to TCAT McMinnville policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. All TCAT McMinnville email information is categorized into four main classifications with retention guidelines:
Administrative Correspondence (4 years)
Fiscal Correspondence (4 years)
General Correspondence (1 year)

Current Hardware Needs cannot be met at this time for the above Policy

3.0 Policy
3.1 Administrative Correspondence
TCAT McMinnville Administrative Correspondence includes, though is not limited to clarification of established company policy, including holidays, time card information, dress code, work place behavior and any legal issues such as intellectual property violations. All email with the information sensitivity label Management Only shall be treated as Administrative Correspondence.

3.2 Fiscal Correspondence
TCAT- McMinnville Fiscal Correspondence is all information related to revenue and expense for the company and must be retained.

3.3 General Correspondence

TCAT- McMinnville General Correspondence covers information that relates to customer interaction and the operational decisions of the business. The individual employee is responsible for email retention of General Correspondence.

3.4 Ephemeral Correspondence

TCAT- McMinnville Ephemeral Correspondence is by far the largest category and includes personal email, requests for recommendations or review, email related to product development, updates and status reports.

3.5 Instant Messenger Correspondence

TCAT- McMinnville Instant Messenger General Correspondence may be saved with logging function of Instant Messenger, or copied into a file and saved. Instant Messenger conversations that are Administrative or Fiscal in nature should be copied into an email message and sent to the appropriate email retention address.

3.6 Encrypted Communications

TCAT- McMinnville encrypted communications should be stored in a manner consistent with TCAT- McMinnville Information Sensitivity Policy, but in general, information should be stored in a decrypted format.

3.7 Recovering Deleted Email via Backup Media

TCAT- McMinnville maintains backup tapes from the email server and once a quarter a set of tapes is taken out of the rotation and they are moved offsite. No effort will be made to remove email from the offsite backup tapes.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Definitions

Terms and Definitions

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within TCAT- McMinnville is done via a license. Please contact the appropriate support organization if you require a license.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of TCAT- McMinnville.

Encryption

Secure TCAT- McMinnville Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow corporate guidelines on export controls on cryptography, and consult your manager and/or corporate legal services for further guidance.

Email policy

The purpose of this policy is to ensure the proper use of The Tennessee College of Applied Technology - McMinnville's email system and make users aware of what The Tennessee College of Applied Technology - McMinnville deems as acceptable and unacceptable use of its email system. The Tennessee College of Applied Technology - McMinnville reserves the right to amend this policy at its discretion. In case of amendments, users will be informed appropriately.

LEGAL RISKS

Email is a business communication tool and users are obliged to use this tool in a responsible, effective and lawful manner. Although by its nature email seems to be less formal than other written communication, the same laws apply. Therefore, it is important that users are aware of the legal risks of email:

- If you send emails with any libelous, defamatory, offensive, racist or obscene remarks, you and The Tennessee College of Applied Technology - McMinnville can be held liable.
- If you forward emails with any libelous, defamatory, offensive, racist or obscene remarks, you and The Tennessee College of Applied Technology - McMinnville can be held liable.
- If you unlawfully forward confidential information, you and The Tennessee College of Applied Technology - McMinnville can be held liable.
- If you unlawfully forward or copy messages without permission, you and The Tennessee College of Applied Technology - McMinnville can be held liable for copyright infringement.
- If you send an attachment that contains a virus, you and The Tennessee College of Applied Technology - McMinnville can be held liable.

By following the guidelines in this policy, the email user can minimize the legal risks involved in the use of email. If any user disregards the rules set out in this Email Policy, the user will be fully liable and The Tennessee College of Applied Technology - McMinnville will disassociate itself from the user as far as legally possible.

LEGAL REQUIREMENTS

The following rules are required by law and are to be strictly adhered to. It is **prohibited** to:

- **Send or forward emails containing libelous, defamatory, offensive, racist or obscene remarks. If you receive an email of this nature, you must promptly notify your supervisor.**
- Forward a message without acquiring permission from the sender first.
- Send unsolicited email messages.
- Forge or attempt to forge email messages.
- Disguise or attempt to disguise your identity when sending mail.
- Send email messages using another person's email account.
- Copy a message or attachment belonging to another user without permission of the originator.

BEST PRACTICES

The Tennessee College of Applied Technology - McMinnville considers email as an important means of communication and recognizes the importance of proper email content and speedy replies in conveying a professional image and delivering good customer service. Users should take the same care in drafting an email as they would for any other communication. Therefore The Tennessee College of Applied Technology - McMinnville wishes users to adhere to the following guidelines:

- **Writing emails**:
    - Write well-structured emails and use short, descriptive subjects.
    - The Tennessee College of Applied Technology - McMinnville's email style is informal. This means that

sentences can be short and to the point. You can start your email with 'Hi', or 'Dear', and the name of the person. Messages can be ended with 'Best Regards'.
    - Signatures must include your name, job title and company name. A disclaimer will be added underneath your signature (see Disclaimer)
    - Users should spell check all mails prior to transmission.
    - Do not send unnecessary attachments. Compress attachments larger than 200K before sending them.
    - Do not write emails in capitals.
    - Do not use cc: or bcc: fields unless the cc: or bcc: recipient is aware that you will be copying a mail to him/her and knows what action, if any, to take.
    - If you forward mails, state clearly what action you expect the recipient to take.
    - Only send emails of which the content could be displayed on a public notice board. If they cannot be displayed publicly in their current state, consider rephrasing the email, using other means of communication, or protecting information by using a password (see confidential).
    - Only mark emails as important if they really are important.
- **Replying to emails**:
    - Emails should be answered within at least 8 working hours, but users must endeavor to answer priority emails within 4 hours.
    - Priority emails are emails from existing customers and business partners.
- **Newsgroups**:
    - Users should consult with the IT department prior to subscribing to Newsgroups
- **Maintenance**:
    - Delete any email messages that you do not need to have a copy of, and set your email client to automatically empty your 'deleted items' on closing.

PERSONAL USE

It is strictly forbidden to use The Tennessee College of Applied Technology - McMinnville's email system for anything other than legitimate business purposes. Therefore, the sending of personal emails, chain letters, junk mail, jokes and executables is discouraged. All messages distributed via the company's email system are The Tennessee College of Applied Technology - McMinnville's property.

CONFIDENTIAL INFORMATION

Never send any confidential information via email. If you are in doubt as to whether to send certain information via email, check this with your supervisor first.

PASSWORDS

All passwords must be made known to the company. The use of passwords to gain access to the computer system or to secure specific files does not provide users with an expectation of privacy in the respective system or document.

ENCRYPTION

Users may not encrypt any emails without obtaining written permission from their supervisor. If approved, the encryption key(s) must be made known to the company.

EMAIL RETENTION

All emails will be deleted after 60 days. If a user has sufficient reason to keep a copy of an email, the message must be moved to the folder 'For archiving'.

EMAIL ACCOUNTS

All email accounts maintained on our email systems are property of The Tennessee College of Applied Technology - McMinnville. Passwords should not be given to other people and should be changed once a month. Email accounts not used for 60 days will be

deactivated and possibly deleted. (Address for Mail Server 198.146.11.3) Email account usernames are the entire email address and can produced at Http://ttcadmin.tbr.edu.

SYSTEM MONITORING

Users expressly waive any right of privacy in anything they create, store, send or receive on the company's computer system. The Tennessee College of Applied Technology - McMinnville can, but is not obliged to, monitor emails without prior notification. If there is evidence that you are not adhering to the guidelines set out in this policy, The Tennessee College of Applied Technology - McMinnville reserves the right to take disciplinary action, including termination and/or legal action.

DISCLAIMER

The following disclaimer will be added to each outgoing email:

Protected by AVG antivirus.

QUESTIONS

If you have any questions or comments about this Email Policy, please contact Administration. If you do not have any questions The Tennessee College of Applied Technology - McMinnville presumes that you understand and are aware of the rules and guidelines in this Email Policy and will adhere to them.

DECLARATION

I have read, understand and acknowledge receipt of the Email policy. I will comply with the guidelines set out in this policy and understand that failure to do so might result in disciplinary or legal action.

Signature: _____ Date: _____

Printed Name: _____

Information Sensitivity Policy

6.0 Purpose
The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of Tennessee College of Applied Technology - McMinnville without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect Tennessee College of Applied Technology - McMinnville Confidential information (e.g., Tennessee College of Applied Technology - McMinnville Confidential information should not be left unattended in conference rooms).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Infosec.

7.0 Scope
All Tennessee College of Applied Technology - McMinnville information is categorized into two main classifications:

- Tennessee College of Applied Technology - McMinnville Public
- Tennessee College of Applied Technology - McMinnville Confidential

Tennessee College of Applied Technology - McMinnville Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to Tennessee College of Applied Technology - McMinnville Systems, Inc.

Tennessee College of Applied Technology - McMinnville Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential acquisition targets, and other information integral to

the success of our company. Also included in Tennessee College of Applied Technology - McMinnville Confidential is information that is less critical, such as telephone directories, general institution information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of Tennessee College of Applied Technology - McMinnville Confidential information is "Tennessee College of Applied Technology - McMinnville Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to Tennessee College of Applied Technology - McMinnville by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into Tennessee College of Applied Technology - McMinnville's network to support our operations.

Tennessee College of Applied Technology - McMinnville personnel are encouraged to use common sense judgment in securing Tennessee College of Applied Technology - McMinnville Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

8.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as Tennessee College of Applied Technology - McMinnville Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the Tennessee College of Applied Technology - McMinnville Confidential information in question.

8.1 **Minimal Sensitivity:** General institution information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "Tennessee College of Applied Technology - McMinnville Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "Tennessee College of Applied Technology - McMinnville Proprietary" or similar labels at the discretion of your individual business unit or department. Even if no

marking is present, Tennessee College of Applied Technology - McMinnville information is presumed to be "Tennessee College of Applied Technology - McMinnville Confidential" unless expressly determined to be Tennessee College of Applied Technology - McMinnville Public information by a Tennessee College of Applied Technology - McMinnville employee with authority to do so.

Access: Tennessee College of Applied Technology - McMinnville employees, contractors, people with a business need to know.
Distribution within Tennessee College of Applied Technology - McMinnville: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Tennessee College of Applied Technology - McMinnville internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.
Electronic distribution: No restrictions except that it be sent to only approved recipients.
Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.
Disposal/Destruction: Deposit outdated paper information in specially marked disposal bins on Tennessee College of Applied Technology - McMinnville premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

8.2 **More Sensitive:** Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "Tennessee College of Applied Technology - McMinnville Confidential" or "Tennessee College of Applied Technology - McMinnville Proprietary", wish to label the information "Tennessee College of Applied Technology - McMinnville Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: Tennessee College of Applied Technology - McMinnville employees and non-employees with signed non-disclosure agreements who have a business need to know.
Distribution within Tennessee College of Applied Technology - McMinnville: Standard interoffice mail, approved electronic mail and electronic file transmission methods.
Distribution outside of Tennessee College of Applied Technology - McMinnville internal mail: Sent via U.S. mail or approved private carriers.
Electronic distribution: No restrictions to approved recipients within Tennessee College of Applied Technology - McMinnville, but should be encrypted or sent via a private link to approved recipients outside of Tennessee College of Applied Technology - McMinnville premises.
Storage: Individual access controls are highly recommended for electronic information.
Disposal/Destruction: In specially marked disposal bins on Tennessee College of Applied Technology - McMinnville premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

8.3 **Most Sensitive:** Trade secrets & marketing, operational, personnel, financial, source code, & technical information integral to the success of our company

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that Tennessee College of Applied Technology - McMinnville Confidential information is very sensitive, you may should label the information "Tennessee College of Applied Technology - McMinnville Internal: Registered and Restricted", "Tennessee College of Applied Technology - McMinnville Eyes Only", "Tennessee College of Applied Technology - McMinnville Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of Tennessee College of Applied Technology - McMinnville Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (Tennessee College of Applied Technology - McMinnville employees and non-employees) designated with approved access and signed non-disclosure agreements.
Distribution within Tennessee College of Applied Technology - McMinnville: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of Tennessee College of Applied Technology - McMinnville internal mail: Delivered direct; signature required; approved private carriers.
Electronic distribution: No restrictions to approved recipients within Tennessee College of Applied Technology - McMinnville, but it is highly recommended that all information be strongly encrypted.
Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer, which at TCAT McMinnville is located in the Server Room.
Disposal/Destruction: Strongly Encouraged: In specially marked disposal bins on Tennessee College of Applied Technology - McMinnville premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.
Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

9.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

10.0 Definitions
Terms and Definitions

Appropriate measures
To minimize risk to Tennessee College of Applied Technology - McMinnville from an outside business connection. Tennessee College of Applied Technology - McMinnville computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access Tennessee College of Applied Technology - McMinnville institution information, the amount of information at risk is minimized.

Configuration of Tennessee College of Applied Technology - McMinnville-to-other business connections
Connections shall be set up to allow other businesses to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required
Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods
Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and stamp it confidential.

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, [insert institution supported mailers here…]. If you have a business need to use other mailers contact the appropriate support organization.

Approved Encrypted email and files
Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. PGP use within Tennessee College of Applied Technology - McMinnville is done via a license. Please contact the appropriate support organization if you require a license.

Company Information System Resources
Company Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge
To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of software on the Miniserver. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On Mac’s and PC's, this includes mandatory screensavers after 10 minutes.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Tennessee College of Applied Technology - McMinnville.

Encryption
Secure Tennessee College of Applied Technology - McMinnville Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow institution guidelines on export controls on cryptography, and consult your manager and/or institution legal services for further guidance.

One Time Password Authentication
One Time Password Authentication on Internet connections is accomplished by using a one-time password token to connect to Tennessee College of Applied Technology -

McMinnville's internal network over the Internet. Contact your support organization for more information on how to set this up.

Physical Security
Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, always use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link
A Private Link is an electronic communications path that Tennessee College of Applied Technology - McMinnville has control over its entire distance. For example, all Tennessee College of Applied Technology - McMinnville networks are connected via a private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. Tennessee College of Applied Technology - McMinnville also has established private links to other companies, so that all email correspondence can be sent in a more secure manner. Companies which Tennessee College of Applied Technology - McMinnville has established private links include all announced acquisitions and some short-term temporary links

Revision History
1/10/2011
11/30/2015

HEOA / P2P File Sharing Policy

Overview

As an addendum to the Tennessee College of Applied Technology - McMinnville's Acceptable Use Policy—which details the utilization of the institution network, the Internet, e-mail, and employees and students' personal computers—this policy prohibits the use of Peer-to-Peer (P2P) file-sharing applications and goes into effect immediately. The Tennessee College of Applied Technology - McMinnville's goal with this additional policy is to:

- Realize the maximum productivity from each employee.
- Address any potential liability from instances when employees and students download copyrighted material.
- Minimize network disruption.
- Protect the network from exposure to malicious code (worm, virus, Trojan horse).
- Protect the Tennessee College of Applied Technology - McMinnville's intellectual property.

Here is an explanation of each issue as it relates to file-sharing applications and our institution:

Employee and Student productivity

The ongoing health of the institution is contingent upon each Employee and Student giving each task his or her maximum attention and effort. Using a file-sharing application to search for files, downloading them onto the institution network or a client machine, and reading or playing them at a workstation is not germane to an employee's and student's job duties and does not enhance a Employee and Student's productivity. Another issue is the possibility that P2P applications could disrupt software on an employee's and student's workstation.

Liability

Although many materials have been placed on P2P networks with a creator's consent, much of the material (images, software, movies, music, video) has been duplicated from copyrighted materials. Downloading such files onto the institution network or a client machine places the institution at significant risk for legal action by the copyright holder and other organizations. File-sharing networks also provide ready access to pornography or other offensive material, subjecting the institution and its employees and students to additional legal risk.

Network disruption

Although the institution has sufficient Internet bandwidth to accommodate all business-related activity, performance can degrade significantly when P2P file-sharing applications are used, especially when large files are being downloaded. This problem is compounded when other users on the P2P network use institution bandwidth to download files from the employee's and student's computer, which can greatly slow other services, such as e-mail, Web browsing, and—more significantly—e-commerce on the institution Web site.

Security

P2P networks can introduce serious gaps in an otherwise secure network. Threats such as worms and viruses can easily be introduced into the Tennessee College of Applied Technology - McMinnville's network. P2P applications, if modified, can also allow users outside the institution to gain access to data on the employee's and student's computer or even the corporate network. (Although most P2P applications allow users to disable file-sharing, such measures do little to prevent threats from being downloaded onto a user's machine.) Some P2P applications will also allow third parties to see the user's IP address. The installation of spyware is also common with many P2P applications.

Protecting the Tennessee College of Applied Technology - McMinnville's intellectual property

The use of P2P file-sharing applications can sometimes allow other members of the P2P network to have access to everything on a local machine, putting the Tennessee College of Applied Technology - McMinnville's intellectual property assets, as well as an employee's and student's personal information, at risk.

Additional Resources

- Check out all of TechRepublic's newsletter offerings.
- "Stop file-sharing applications on your network" (TechRepublic)
- "CA slaps spyware label on Kazaa" (TechRepublic)
- "See how this IT group identified a P2P bandwidth utilization problem" (TechRepublic)
- "How can you avoid peer-to-peer security nightmares?" (TechRepublic)
- "Take precautions against peer-to-peer threats" (TechRepublic)

Communications Assistance for Law Enforcement Act (CALEA)

(Summary: The right to monitor and cooperate with Law Enforcement on Data usage within an organization such as the internet and email.)

Note: The following information is provided for general reference purposes only and should not be relied upon for a full and complete understanding of the CALEA statute. Carriers and others seeking to know how they are affected by CALEA should consult the statute and relevant FCC rules, Orders, and other publications, as well as rules and other documents published by the United States Department of Justice and the Federal Bureau of Investigation (FBI).

CALEA compliance is a legal obligation imposed on all carriers covered by the statute. To assist carriers with designing a schedule for becoming CALEA-compliant, the FBI has developed a carrier Flexible Deployment Assistance program for circuit mode compliance. Note that this program has been discontinued for packet mode extension requests. The FCC encourages all carriers to consult with the FBI about program details. Detailed instructions and contact information for this program, as well as summary information about current CALEA compliance requirements, may be obtained online from the FBI/CIS: http://www.askcalea.net.

Report complaints and potential violations to:
Dr. Warren Laux, Director - warren.laux@TCAT McMinnville.edu
Marvin Lusk – marvin.lusk@tcatmcminnville.edu
Mike Garrison, Student Services Coordinator - mike.garrison@TCAT McMinnville.edu
Debra Akers, IT Manager – debra.akers@TCAT McMinnville.edu
Jerry Parker, Asst. IT Manager – jerry.parker@TCAT McMinnville.edu

COPPA

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, e-mail address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information -- for example, hobbies, interests and information collected through cookies or other types of tracking mechanisms -- when they are tied to individually identifiable information. More information can be found here. (http://www.ftc.gov/bcp/conline/pubs/buspubs/coppa.htm)

The information provided for COPPA is for any forums established by TCAT McMinnville.

STUDENT NOTIFICATION OF RIGHTS

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

Students of the Tennessee College of Applied Technology - McMinnville have legal rights under the Family Educational Rights and Privacy Act (FERPA) of 1974, as well as the related regulations of the Department of Education. This law, also referred to as the Buckley Amendment, and the regulations provide that:

- A student has a right to inspect and review their educational records by submitting a written request to the Student Records Clerk. Within 30 days of the request, the Student Records Clerk will notify the student of the date and time when the records can be inspected.

- A student may request that any record be amended if the student believes it is inaccurate, misleading, or otherwise in violation of privacy rights. To request an amendment, the student must write the school official responsible for the record and clearly specify why it is inaccurate or misleading. If the school decides not to amend the record, the student will be notified of his/her rights to a school hearing. Additional information regarding hearing procedures will be provided to the student at that time.

- The Tennessee College of Applied Technology - McMinnville will obtain the student's written consent before disclosing personally identifiable information about the student from their records, unless the consent is not required by the law or the regulations. One exception which permits disclosure without consent is disclosure to school officials with legitimate educational interests. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her responsibility. A school official is a person employed by the institution in an administrative, supervisory, faculty or staff position; a person or company with whom the school has contracted services; a member of the school's governing board, or a student serving in an official capacity, such as student review hearings. Upon request, the school also discloses education records without consent to officials of another school in which a student seeks or intends to enroll, but will notify the student, if possible, of this request.

- If a student wishes to authorize the release of records to other individuals, the student must complete the "Authorization to Release Information" form, available in the Student Records Office. For security purposes, photo identification will be required in order to complete this form.

- Directory information such as name, address, date of birth, telephone listing, course of study, dates of attendance, awards earned, etc. may be disclosed unless

the student submits a written request that such information not be disclosed. If a student wishes to restrict the release of directory information to outside agencies and schools, a "Confidentiality of Records" form must be completed and submitted to the Student Records Office.

- A student has the right to file a complaint with the U.S. Department of Education concerning alleged failures by the institution to comply with the requirements of FERPA. Contact information is provided below:

Family Policy Compliance Office
U.S. Department of Education
600 Independence Avenue, SW
Washington, DC 20202-4605

GLBA (The Gramm-Leach-Bliley Act)

The Gramm-Leach-Bliley Act (GLBA) was signed into law in 1999 and directly affects financial institutions, including insurance companies and agencies. At the heart of GLBA is a requirement that financial institutions provide a privacy notice to their customers and restrict what non-public personal information (NPI) they share about customers with third parties. Financial institutions are also required to provide security and integrity of customers' NPI by way of physical and electronic means.

While Tennessee College of Applied Technology - McMinnville is primarily an educational institution and its areas covered by GLBA are few, the Technology Center is committed to satisfying the law in all its financial processes. This site provides detailed information on Technology Center policies and procedures designed to facilitate compliance with GLBA.

Report complaints and potential violations to :
Dr. Warren Laux, Director- warren.laux@TCAT McMinnville.edu
Mike Garrison, Student Services Coordinator- mike.garrison@TCAT McMinnville.edu
Debra Akers, IT Manager- debra.akers@TCAT McMinnville.edu

GLBA: Who's Covered?

Administration

Office of Financial Aid (Student Services)

Office of Information Technology (Electronic Records-Student Information Management)

GLBA: Required Information Security Program

PROGRAM: Gramm-Leach-Bliley Act (GLBA) Required Information Security Program

STATEMENT: This document summarizes the Tennessee College of Applied Technology - McMinnville's comprehensive written information security program mandated by the Federal Trade Commission's Safeguards Rule and the Gramm–Leach–Bliley Act (GLBA).

APPLICABILITY: The GLBA Information Security Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with Tennessee College of Applied Technology - McMinnville, whether in paper, electronic or other form, which is handled or maintained by or on behalf of Tennessee College of Applied Technology - McMinnville or its affiliates. For these purposes, the term nonpublic financial information shall mean any information (i) a

student or other third party provides in order to obtain a financial service from Tennessee College of Applied Technology - McMinnville, (ii) about a student or other third party resulting from any transaction with Tennessee College of Applied Technology - McMinnville involving a financial service, or (iii) otherwise obtained about a student or other third party in connection with providing a financial service to that person.

DEFINITIONS:
Financial Service: A "Financial Service" is defined by federal law to include, but not be limited to, such activities as the lending of money; investing for others; providing or underwriting insurance; giving financial, investment or economic advisory services; marketing securities and the like.

GUIDING PRINCPLES/PURPOSE: In particular, this document describes the elements of the GLBA Information Security Program pursuant to which Tennessee College of Applied Technology - McMinnville intends to (i) ensure the security and confidentiality of covered records, (ii) protect against any anticipated threats or hazards to the security of such records, and (iii) protect against the unauthorized access or use of such records or information in ways that could result in substantial harm or inconvenience to customers. The GLBA Information Security Program incorporates by reference Tennessee College of Applied Technology - McMinnville's policies and procedures enumerated below, and is in addition to any institutional policies and procedures that may be required pursuant to other federal and state laws and regulations, including, without limitation, FERPA.

RESPONSIBILITY (IES): Tennessee College of Applied Technology - McMinnville's Technology Center IT Manager (IT Manager) with overall responsibility for overseeing Technology Center information security is responsible for coordinating and overseeing the information security program. Consistent with the Technology Center Information Security Policy, the IT Manager may designate other representatives of Tennessee College of Applied Technology - McMinnville to oversee and coordinate particular elements of the GLBA Information Security Program. Any questions regarding implementation or the interpretation of this document should be directed to the IT Manager or his/her designees.

ADMINISTRATION AND IMPLEMENTATION:

1. Risk Identification and Assessment. Tennessee College of Applied Technology - McMinnville intends, as part of the GLBA Information Security Program, to undertake to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. In implementing the GLBA Information Security Program, the IT Manager or his/her designee will establish procedures for identifying and assessing such risks in each

relevant area of Tennessee College of Applied Technology - McMinnville's operations, including:

• Employee training and management. The IT Manager will coordinate with representatives in Tennessee College of Applied Technology - McMinnville's Financial Aid offices to evaluate the effectiveness of the Technology Center's procedures and practices relating to access to and use of student records, including financial aid information. This evaluation will include assessing the effectiveness of Tennessee College of Applied Technology - McMinnville's current policies and procedures in this area, including:

Release of Student Information Policy

• Information Systems and Information Processing and Disposal. The IT Manager will assess the risks to nonpublic financial information associated with Tennessee College of Applied Technology - McMinnville's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. These risks will be evaluated in view of Tennessee College of Applied Technology - McMinnville's Computer Systems Acceptable Use Policy, the Technology Center Information Security Policy and the Records Retention Policy.

• Detecting, Preventing and Responding to Attacks. Consistent with the provisions of the Technology Center Information Security Policy, the IT Manager and/or his/her designee will evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. The IT Manager may elect to delegate to local information security personnel the responsibility for monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by Tennessee College of Applied Technology - McMinnville.

2. Designing and Implementing Safeguards. The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The IT Manager, in collaboration with the Tennessee Board of Regents, will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures.

3. Overseeing Service Providers. The IT Manager or his/her designee shall coordinate with those responsible for the third party service procurement activities among IT and other affected departments to raise awareness of, and to institute methods for,

selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the IT Manager will work with the Tennessee Board of Regents, Administration and Student Services to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. Any deviation from these standard provisions will require the approval of the Tennessee Board of Regents.

4. Adjustments. The IT Manager is responsible for evaluating and adjusting the GLBA Information Security Program based on the risk identification and assessment activities undertaken, as well as any material changes to Tennessee College of Applied Technology - McMinnville's operations or other circumstances that may have a material impact it.

ENFORCEMENT:
As described in the Technology Center Information Security Policy, anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of services or termination of employment.

RESOURCE(S)
The Technology Center Information Security Policy, the Records Retention Policy and Computer Systems Acceptable Use Policy.

REVIEW CYCLE:
This program will be reviewed and updated as needed, at least annually, based on the recommendations of the Technology Center IT Manager or Director.

TRAINING:
Faculty and Staff will review confidentiality policies and procedures and be trained on an annual basis.

PROTECTION:
All records will be locked in a secure room and will be locked in filing cabinets. All Electronic records will be locked in the server room. Access will only be granted to Administration, Student Services or the IT Department. All Electronic records are protected by a Disaster Recovery Program that includes the use of NAT, Firewalls and Network Intrusion Detection to include logging on each computer. Any breach will be reported to the Director or Student Services Immediately.

<u>Conference Report and Text of Gramm-Leach-Bliley Bill</u>
U.S. Senate Committee on Banking, Housing, and Urban Affairs

Financial Services Modernization Act — Summary of Provisions
U.S. Senate Committee on Banking, Housing, and Urban Affairs

HIPAA

BRIEF SUMMARY (Information Technology Department)

WHAT IS HIPAA?

HIPAA stands for the Health Insurance Portability and Accountability Act of 1996. A major component of HIPAA addresses the privacy of individuals' health information by establishing a nation-wide federal standard concerning the privacy of health information and how it can be used and disclosed. This federal standard will generally preempt all state privacy laws except for those that establish stronger protections. The HIPAA privacy laws are effective **April 14, 2003**.

Generally, HIPAA "covered entities" will have to comply with HIPAA rules for any health or medical information of identifiable individuals, including their medical records, medical billing records, any clinical or research databases, and tissue bank samples. Covered entities are health care providers, health plans (including employer's sponsored plans), and healthcare clearing houses (e.g., billing agent). Records maintained at the Tennessee College of Applied Technology - McMinnville are kept secure and are only disclosed in emergencies and to the individual owners.

Report complaints and potential violations to:
Dr. Warren Laux, Director - warren.laux@TCAT McMinnville.edu
Mike Garrison, Student Services Coordinator - mike.garrison@TCAT McMinnville.edu
Debra Akers, IT Manager – debra.akers@TCAT McMinnville.edu
Jerry Parker, Asst. IT Manager – jerry.parker@TCAT McMinnville.edu

FISMA (Federal Information Security Management Act)

The FISMA Implementation Project was established in January 2003 to produce several key security standards and guidelines required by Congressional legislation. These publications include FIPS 199, FIPS 200, and NIST Special Publications 800-53, 800-59, and 800-60. Additional security guidance documents are being developed in support of the project including NIST Special Publications 800-37, 800-39, and 800-53A. It should be noted that the Computer Security Division continues to produce other security standards and guidelines in support of FISMA. These publications can be located by visiting the division's Publications page at: http://csrc.nist.gov/publications/.

The Tennessee College of Applied Technology - McMinnville is committed to privacy and security of all electronic records. Through encryption and practicing Disaster Recovery and Planning, the IT department follows guidelines set forth under the FISMA Act.

Privacy Information

The TCAT-McMinnville Information Technology Department protects the privacy of students and clients of TCAT- McMinnville. Information collected and stored on servers is shared only with the following TCAT- McMinnville Personnel and outside sources.

- Staff (Limited to attendance and personal information needed for classroom functionality)
- Student Services (Unlimited)
- Administration (Unlimited)
- Outside Sources (Limited by singed/verbal release authorized by the student or owner of the information)

The Tennessee College of Applied Technology - McMinnville at McMinnville will conform to laws such as Gramm-Leech and Bliley, HIPAA and other Federal and State laws as applicable.

VITAL RECORDS POLICY (GS-070)

All Tennessee College of Applied Technology - McMinnville records designated as vital or essential to the operation of the Tennessee College of Applied Technology - McMinnville and which if destroyed would seriously impair or disrupt normal Tennessee College of Applied Technology - McMinnville affairs, or which by their loss might place the TCAT in a state of legal or fiscal jeopardy, are to be secured electronically ***if possible*** or other comparable and suitable method.

Files not stored electronically will be stored in a secure location and is the responsibility of Student Services or Administration.

RESPONSIBILITY FOR PROTECTION OF VITAL RECORDS

Tennessee College of Applied Technology - McMinnville Information Technology Department that have records designated as vital records have the primary responsibility to keep these records secure on a current basis.

DESIGNATED ELECTRONIC RECORDS

Following is a listing of records that must be secured as outlined above (IF ELECTRONIC). See TBR sections:
Student Academic Records
Student Admission Files
Student Loan Notes
Tennessee College of Applied Technology - McMinnville Leases and Contracts
Land Deed Files and Easements
Medical and Dental Information Files
Engineering Drawings of Tennessee College of Applied Technology - McMinnville Buildings
(Original and As-Built)
Construction Specifications Files
Psychological Testing & Counseling Files
Accounting Records
Personnel Records (Human Resources)

Revisions and Publication

Revised: 11/30/15

IT Policy is published to TCAT McMinnville Website with IP addresses and other sensitive data omitted.

A hard copy of the IT Policy is made available for distribution to any student, faculty, or staff member in the Student Services Office with IP addresses and other sensitive data omitted.

The following statement with the school logo is the wallpaper for all computers attached to the TCAT McMinnville.edu domain and student.ttcmcminnville.edu domain:

"By using this computer you are agreeing to comply with the Tennessee College of Applied Technology McMinnville and Tennessee Board of Regents IT Policies and Usage Agreements"

IT Policy emailed to the Oversight Committee on 12/15/2015 for review.