Information Technology Policies and Procedures Plan

TENNESSEE COLLEGE OF APPLIED TECHNOLOGY MCMINNVILLE

WWW.TCATMCMINNVILLE.EDU

Table of Contents

TCAT McMinnville Computer and Network Policies

Exhibits

Introduction:

The Tennessee College of Applied Technology McMinnville (TCAT McMinnville) Information Technology (IT) Policy and Procedure Manual provides the policies and procedures to be followed by all faculty and staff for the selection and use of IT resources within the college. It also provides the guidelines that TCAT McMinnville will use to administer these policies, with the correct procedures to follow.

Policy:

TCAT McMinnville will attempt to keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. This policy is evaluated annually and revised as necessary by a policy evaluation committee composed of staff/faculty for revisions and approval. These policies are available to all faculty and staff and as changes or amendments are made by the group. This policy is kept in the IT office. These policies and procedures apply to all TCAT McMinnville and satellite campus employees.

IT Staff and Instructors:

Jessica Gammon
Computer Information Technology Associate Instructor / IT Specialist
jessica.gammon@tcatmcminnville.edu

Dave McDonald
Computer Information Technology Adjunct Instructor
james.mcdonald@tcatmcminnville.edu

Description of IT Environment
Network Setup – Infrastructure

The TCAT McMinnville's Information Technology Department is responsible for the upkeep and maintenance on the Local Area and Wireless Networks.

McMinnville Campus

a. 1g Fiber Internet provided through Ben Lomand Connect
b. Fortinet 101E Firewall
c. 20 Dell Managed Switches
d. 13 Aerohive Wi-Fi access points
e. 1g fiber ethernet connecting all switches

Manchester Campus

a. 1g Fiber Internet provided by Ben Lomand Connect
b. 100F Fortinet FW
c. 2 Aerohive Wi-Fi access points
d. 1 Dell N2048P switch

1. Acceptable Computer Use Policy

Compliance with this computer usage policy is necessary to ensure maximum utilization and performance of each computer system as well as provide a sense of security and restful cooperation among the school community. Strict adherence to this policy will prevent costly damage or repair, downtime, and loss of computer privileges.

- No computer system can be used without prior approval of the supervising instructor or other school official.
- Because software is protected under copyright laws, no software can be copied without written authorization.
- No outside software can be loaded on school computers without written approval.
- Changes to a system's configuration or the inappropriate deleting or changing of computer settings is forbidden.
- Technical manuals may not be removed from the training area.
- Computers must not be moved or repositioned on tables.
- To prevent damage to any system, computer users should not eat or drink within five (5) feet of a computer system, or smoke or vape around computer equipment.

Specific policy for access to the Internet:

- The system may not be used for personal or private matters.
- Creating, distributing, or accessing hate mail, pornographic or obscene materials, discriminatory, or harassing materials, is strictly forbidden.
- Anti-social behaviors, including spamming are forbidden.
- Creating, distributing, or accessing confidential material, including but not limited to, test files or student/personnel records are forbidden.
- IMPORTANT NOTE: Any person who violates this policy will be subject to appropriate disciplinary sanction, including dismissal and/or possible prosecution. (See TBR Policy 3:02:00:01 regarding Student Conduct and Disciplinary Sanctions)

Copyright and Digital Millennium Act:

Materials published by the Tennessee College of Applied Technology-McMinnville are protected by the Digital Millennium Copyright Act. The DMCA also requires that the institution inform all computer and network users that downloading of copyrighted material is prohibited. In addition, Tennessee Code Annotated §49-7-1(c) specifies that the institution ensure that no copyrighted digital music or videos be downloaded using institutional resources. Any attempts to do so will result in appropriate actions.

Violations:
Violations of the policy will result in action by the appropriate institution office. Students who violate this policy will be referred to the Coordinator of Student Services for appropriate action. Employees who violate this policy may be subject to disciplinary measures imposed by their supervisor in conjunction with the institution's administration. Violations of local, state or federal laws regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.

Inspection of Electronic Records:
Electronic records sent, received, or stored on computers owned, leased, or administered by the Tennessee College of Applied Technology McMinnville are the property of the College and the Tennessee Board of Regents. As the property of Tennessee College of Applied Technology McMinnville and Tennessee Board of Regents, the content of such records, including electronic mail, are subject to inspection by TCAT McMinnville personnel. Users should have no reasonable expectation of privacy in the use of these resources.

2. Copyright and Digital Millennium Act

Copyright is a form of protection provided by the laws of the United States (Title 17, U.S. Code) to creators of "original works of authorship" including literary, dramatic, musical, artistic, and other published and unpublished works, when "fixed in a tangible form of expression." Protections last for the term of the author's life plus 50 years after death. It is given to individual, group, or corporate authors and to "works for hire". It is illegal for anyone to violate any of the rights provided to the owner of a copyright. The Copyright Act (1976) contains provisions prescribing damages that can be assessed if infringements are committed. In civil cases, the law allows the assessment of actual damages or statutory damages. For each infringement, statutory damages range from $250 to $10,000. These rights, however, are limited in scope. Sections 107-118 of the Copyright Act establish limitations that in some cases are specified as exemptions from liability. One major limitation is the doctrine of "fair-use" which is given statutory basis in Section 107 of the Act.

Violations:
Violations of the policy will result in action by the appropriate institution office. Students who violate this policy will be referred to the Coordinator of Student Services for appropriate action. Employees who violate this policy may be subject to disciplinary measures imposed by their supervisor in conjunction with the institution's administration. Violations of local, state or federal laws regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.

3. Hardware/Software Change Control

All change requests should be logged whether approved or rejected and the results thereof should be documented on a Hardware-Software Change Request Form (**Exhibit C**).
A documented audit trail containing relevant information should be always maintained. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

Types of Changes
There are three types of changes based on approvals needed through the change management process.

1. **Standard Change** – A relatively low-risk change with well-understood outcomes that are regularly made during the course of business. A standard change follows pre-determined processes, is pre-approved by change management processes and may be made at the discretion of an individual employee, provided it has been defined as Standard per the Change Management assessment process, i.e. a server OS upgrade.

2. **Significant Change** – A significant change is one that has medium to high risk for critical services, involves less understood risks, has less predictable outcomes, and/or is a change that is not regularly made during the course of business. Because of the ability to affect downstream or upstream services, any proposed significant change should be reviewed by the Policy/Change Review committee and authorized by at least one of the committee members.

3. **Emergency Change** – This is similar to a Significant Change but must be executed with utmost urgency. There may be fewer people involved in the change management process review, and the change assessment may involve fewer steps, but any emergency change must still be authorized by the Policy/Change Review committee, even in cases where the Policy/Change Review committee cannot review the change in advance.

4. Patch Management

Workstations
Desktops and laptops should have automatic updates enabled for operating system patches. This is the default configuration for all workstations.

Servers
Servers must comply with the minimum baseline requirements that have been approved by the Global Security Office of the Security and Exchange Commission (GSO). 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 assets and the data that resides on the system. They are:

1. Patch and Update the OS
    a. Create a patching process
    b. Identify vulnerabilities and applicable patches
    c. Install permanent fixes

2. Configure the OS to address security adequately
    a. Remove unnecessary service, application, and network protocols
    b. Configure OS user Authentication
    c. Configure resource controls appropriately
3. Install and configure additional security controls if needed
    a. Anti-malware
    b. Intrusion detection
    c. Firewalls

4. Test the security of the OS
    a. Possible impact of the production server
    b. PII information

5. Logging and Monitoring

Approved and standard configuration templates shall be used when deploying server systems to include:

a. All Administrator actions should be logged.
b. Host security agents such as antivirus should be monitored.
c. Network scans to verify only required network ports and network shares are in use.
d. Verify administrative group membership.
e. User Access Control

Policy Statement
TCAT McMinnville will establish specific requirements for protecting information and information systems against unauthorized access.

Definition
Access control rules and procedures are required to regulate who can access TCAT McMinnville's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing TCAT McMinnville's information in any format, and on any device.

6. User Access Control

Formal user access control procedures should be documented, implemented, and kept up to date for each application and information system to ensure authorized user access and to prevent unauthorized access. They should cover all stages of the lifecycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access. Each user should be allocated access rights and permissions to computer systems and data that:

a. Are commensurate with the tasks they are expected to perform.
b. Have a unique login that is not shared with or disclosed to any other user.
c. Have an associated unique password that is requested at each new login.

User access rights should be reviewed at regular intervals to ensure that the appropriate rights are still allocated. System administration accounts should only be provided to users that are required to perform system administration tasks.

User Registration
A request for access to the TCAT McMinnville's computer systems must first be submitted to the IT department for approval. Access must only be given if approval has been gained from the IT department.

When an employee leaves TCAT McMinnville, their access to computer systems, Banner and email should be suspended at the close of business on the employee's last working day.

User Responsibilities

It is a user's responsibility to prevent their user-ID and password from being used to gain unauthorized access to the TCAT-McMinnville's systems by:

a. Following the Password Policy Statements outlined above.
b. Ensuring that any PC they are using that is left unattended is locked or logged out.
c. Leaving nothing on the display that may contain access information such as login names and passwords.
d. Informing the IT Coordinator of any changes to their role and access requirements.

Network Access Control

The use of modems on non-TCAT McMinnville owned PCs connected to the TCAT McMinnville's network can seriously compromise the security of the network. The normal operation of the network must not be interfered with. Specific approval must be obtained from the IT Specialist before connecting any equipment to the TCAT McMinnville's network.

Operating System Access Control

Access to operating systems is controlled by a secure login process. The access control defined in the User Access Management section and the Password section below must be applied. The login procedure must also be protected by limiting the number of unsuccessful attempts, (5), and locking the account if exceeded. The TBR Help Desk (615-366-4444) must be contacted to allow accounts to be unlocked.

All access to operating systems is via a unique login identification (Employee or Student S#) that will be audited and can be traced back to each individual user. The login identification must not give any indication of the level of access that it provides to the system (e.g. administration rights).

System administrators must have individual administrator accounts that can be logged and audited. The administrator account should not be used by individuals for normal day-to-day activities.

TBR Password Guidelines

A weak password is one which is easily discovered, or detected, by people who are not supposed to know it. Examples of weak passwords include words picked out of a dictionary, names of

children and pets, car registration numbers and simple patterns of letters from a computer keyboard.
A strong password is a password that is designed in such a way that it is unlikely to be detected by people who are not supposed to know it, and difficult to work out even with the help of a computer.
Everyone must use strong passwords with a minimum standard of:

a. Must be a minimum of 16 characters.
b. It must include a complex combination of characters as follows:
    - Use at least 1 character from 3 of the 4 following categories: Upper case, Lower case, Numbers (0-9), Symbols.
    - The following are acceptable symbols: @ # $ % ^ - ! + = [ ] { } | \ : ‘ , . ? / ` ~ “( ) ;< > or a blank space

c. Cannot use one of your last 24 passwords.
d. It is of utmost importance that the password remains protected at all times. Never reveal your passwords to anyone.
e. Never use the 'remember password' function.
f. Never write your passwords down or store them where they are open to theft.
g. Never store your passwords in a computer system without encryption.
h. Do not use any part of your username within the password.
i. Do not use the same password to access different TCAT McMinnville systems.
j. Do not use the same password for systems inside and outside of work.

Changing Passwords
Azure AD or Microsoft 365 does not require passwords to be changed but does require 2 factor authentication through text, alternate email or Microsoft Authenticator App. If you become aware, or suspect, that your password has become known to someone else, you must change it immediately and report your concern to the TCAT McMinnville IT Specialist.

System Administration Standards
The password administration process for individual TCAT McMinnville systems is well-documented and available to designated individuals.
All TCAT McMinnville IT systems will be configured to enforce the following:

a. Authentication of individual users, not groups of users - i.e. no generic accounts.
b. Protection with regards to the retrieval of passwords and security details.
c. System access monitoring and logging - at a user level.

Application and Information Access
Access within software applications must be restricted using the security features built into the individual product. The IT Specialist of the software application is responsible for granting access to the information within the system. The access should:

a. Be compliant with the User Access Management section and the Password section above.
b. Be separated into clearly defined roles.
c. Give the appropriate level of access required for the role of the user.
d. Be free from alteration by rights inherited from the operating system that could allow unauthorized higher levels of access.
e. Be logged and auditable.

Policy Compliance
If any user is found to have breached this policy, they may be subject to TCAT McMinnville's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s).
If you do not understand the implications of this policy or how it may apply to you, seek advice from the IT Specialist.

7. User Access

Access to information must be specifically authorized in accordance with TCAT McMinnville's Access Control policy. Access to information will be controlled on the basis of business and security requirements, and access control rules defined for each information system. All TCAT McMinnville users should be allowed to access only those critical business information assets and processes which are required for performing their job duties. Access to critical business information assets and activation of user accounts for contractors, consultants, temporary workers, or vendor personnel must only be in effect when the individual is actively performing service for TCAT McMinnville. Access for contractors, consultants, or vendor personnel to TCAT McMinnville critical business information assets will be provided only on the basis of a contractual agreement.

8. Email Usage

Prohibited Use
The TCAT McMinnville email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any TCAT

McMinnville employee should report the matter to their supervisor immediately. TCAT McMinnville email is managed by TBR IT through Microsoft Outlook 365.

Personal Use
Using a reasonable amount of TCAT McMinnville resources for personal emails is acceptable, but non-work related email shall be saved in a separate folder from work related email. Sending chain letters or joke emails from a TCAT McMinnville email account is prohibited. Mass mailings from the TCAT McMinnville email system shall be approved by TCAT McMinnville Administration before sending. These restrictions also apply to the forwarding of mail received by a TCAT McMinnville employee.

Monitoring
TCAT McMinnville employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. TBR IT may monitor messages without prior notice.

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

9. Disaster Recovery

On all desktop PCs and mobile devices, user data is backed up in the cloud through OneDrive. All hard drives are required to be encrypted through Azure Active Directory Policy managed by TBR IT Staff. The login is done though Azure Active Directory using the employee or student S# or (Portal ID) and secure multifactor authentication password. Banner student information system is housed on TBR servers at various locations and managed by TBR IT staff. Email is housed on Microsoft servers at various locations and is protected by S# or Portal Login with Multifactor Authentication. All campuses use the same guidelines using Azure Active Directory and OneDrive. In the event a PC or mobile device is damaged, the user will be given a new device and if internet access is restored, or they are at another site, they would sign in with their S# or (Portal ID) and secure multifactor authentication password. User files will be restored from OneDrive backup. Student records are stored on TBR Portal servers. No records are kept locally.

Recovery Phases
Recovery activities will be conducted in a phased approach. The emphasis will be to recover the critical applications effectively and efficiently. Critical applications will be recovered over a period of time after data center activation.

Phase I
Move operations to the Disaster Recovery Backup Site, if applicable. This activity will begin with activation of the Disaster Recovery Plan. There is a period of up to 24 hours allowed for organization and the turnover of the disaster recovery backup site.

Phase II
To recover critical business functions, restoration of the critical applications, and critical network connectivity. The goal here is to recover the systems and network so that our staff/faculty/students can continue business and learning.

Phase III
Return data processing activities to the primary facilities or another computer facility, if applicable. The following conditions, if met, will constitute a successful recovery effort:

a. Restore critical applications to the most current date available. Updating the systems and databases will take place as the recovery effort progresses.
b. It is understood that, due to the emergency or disaster, response times will probably be slower than normal production situations.

The Plan provides recovery procedures to be used at the TCAT McMinnville site after repairs have been made.

10. Desktop Computer Security/Usage

The following general guidelines are relevant for all users, no matter what operating system is being used:

a. Maintain up to date and properly configured anti-virus software. Windows machines which are on campus must use Windows Defender ATP. Be sure that real-time protection scans all files.
b. Don't open any e-mail attachments unless you know the sender AND know that it was intentionally sent to you.
c. If you share any files from your machine (not recommended in most cases), be certain that access is protected with a complex password.

11. Mobile Device Security/Usage

Appropriate measures should be taken when using mobile devices to ensure the confidentiality, integrity, and availability of sensitive information, including personally identifiable information

(PII) and that access to sensitive information is restricted to authorized users. Appropriate measures must also be taken to reduce the likelihood of physical loss or damage to mobile devices in order to protect TCAT McMinnville's capital assets. All data stored on desktop and mobile devices must be stored in the Tennessee Board of Regents folder that is synced to Microsoft OneDrive.

Mobile devices include: laptops, smartphones, tablets, and authorized home laptops accessing the TCAT McMinnville network. The same general guidelines for desktop computers apply to TCAT McMinnville's mobile devices. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

12. Server Security/Usage

General Configuration Guidelines:

a. Operating System configuration should be in accordance with approved SANS (**S**ysAdmin, **A**udit, **N**etworking, and **S**ecurity) Institute guidelines listed below.
b. Services and applications that will not be used should be disabled where practical.

13. Server Audit Policy

The purpose of this policy is to ensure all servers deployed at TCAT McMinnville are configured according to the TCAT McMinnville security policies. Servers deployed at TCAT McMinnville shall be audited at least semi-annually and as prescribed by applicable regulatory compliance.

Audits may be conducted to:

a. Ensure integrity, confidentiality and availability of information and resources.
b. Ensure conformance to TCAT McMinnville security policies.

Guidelines

Audits used when deploying server systems are to include but, not limited to:

a. All system logs shall be reviewed on a regular basis
b. All Administrator actions should be logged
c. Windows Updates should be downloaded and applied
d. Authentication restrictions for login
e. Password Complexity Restrictions to deter unauthorized access
f. All File Sharing permissions checked

g. Host security agent such as antivirus must be installed and updated
h. Verify the presence of Anti-Malware
i. Network scans to verify only required network ports and network shares are in use
j. Verify administrative group memberships

14. Network Remote Access and VPN

Remote Access
It is the policy of TCAT McMinnville that mobile computing and storage devices containing or accessing the information resources at TCAT McMinnville must be approved prior to connecting to the information systems at TCAT McMinnville. This pertains to all devices connecting to the network at TCAT McMinnville, regardless of ownership.

Mobile computing and storage devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), Universal Serial Bus (USB) port devices, Compact Discs (CDs), Digital Versatile Discs (DVDs), flash drives, modems, handheld wireless devices, wireless networking cards, and any other existing or future mobile computing or storage device, either personally owned or TCAT McMinnville owned, that may connect to or access the information systems at TCAT McMinnville. A risk analysis for each new media type should be conducted and documented prior to its use or connection to the network at TCAT McMinnville unless the media type has already been approved by the IT department.
Portable computing devices and portable electronic storage media that contain confidential, personal, or sensitive TCAT McMinnville information must use encryption or equally strong measures to protect the data while it is being stored.

Unless written approval has been obtained from the IT department, databases or portions thereof, which reside on the network at TCAT McMinnville, must not be downloaded to mobile computing or storage devices.

Technical personnel and users, which include employees, consultants, vendors, contractors, and students, shall have knowledge of, sign, and adhere to the Acceptable Use of Computers/Internet agreement (**Exhibit A**).

Azure Virtual Private Network (VPN) Access
Approved TCAT McMinnville employees may utilize the benefits of VPNs. Azure VPN access is managed and monitored by TBR IT. Additionally:

a. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to TBR secure networks
b. VPN access is accessed thru Microsoft Azure.

c. When actively connected to the corporate network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
d. Users of computers that are not TCAT McMinnville owned equipment must configure the equipment to comply with TBR VPN and Network policies.
e. Only TCAT McMinnville approved VPN clients may be used. (Azure VPN)
f. 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 TCAT McMinnville Security Policies.
g. Azure VPN is accessed by single sign on which is the same user and password used for Portal Login.

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

15. Wireless Access

This policy prohibits access to TCAT McMinnville's 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 IT department, are approved for connectivity to TCAT McMinnville's networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of TCAT McMinnville's internal networks. This includes any form of wireless communication device capable of transmitting packet data.

Register Access Points and Cards
All third-party wireless Access Points connected to the institution network are a clear violation of policy. All wireless Network Interface Cards (i.e., PC cards) used in institution laptop or desktop computers must be registered with The IT Department.

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

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

16. Computer Incident Response

1. The person who discovers an incident will call the IT Specialist, immediately, listing the possible sources of those who may have discover the incident. The known sources should be provided with a contact procedure and contact list. Sources requiring contact information may be:
    a) Helpdesk
    b) A system administrator
    c) A coordinator
    d) The security department or a security person.

2. If the person discovering the incident is a member of the IT department or affected department, they will proceed to step 5.

3. If the person discovering the incident is not a member of the IT department or affected department, they will call the IT Specialist. (Incident Report Form, **Exhibit B**) will be completed.

4. The IT department will log:
    a) The name of the caller.
    b) Date/Time of the call.
    c) The physical location of the incident.
    d) What equipment or persons were involved?
    e) Location of equipment or persons involved.
    f) Type of Incident.
    g) How the incident was detected.
    h) IP Address of the affected equipment.
    i) IP Address of Source (if known).
    j) Host name and how many Hosts are affected.
    k) Operating System.
    l) When the event was first noticed that supported the idea that the incident occurred.

5. If a data breach occurs, the IT Specialist or affected department staff member will refer to their contact list for both management personnel to be contacted and incident response members to be contacted. The IT Specialist will contact TBR. (TCAT McMinnville IT

Specialist - Jessica Gammon, 931-999-6425). The staff member will log the information received in the same format as the IT Specialist in the previous step. The staff member could possibly add the following:

a) Is the equipment affected business critical?
b) What is the severity of the potential impact?
c) Name of system being targeted, along with operating system, IP address, and location.
d) IP address and any information about the origin of the attack.

6. The IT Specialist will use forensic techniques, including reviewing system logs, looking for gaps in logs, reviewing intrusion detection logs, and interviewing witnesses and the incident victim to determine how the incident was caused. Only authorized personnel should be performing interviews or examining evidence, and the authorized personnel may vary by situation and the organization.

7. The IT Specialist will recommend changes to prevent the occurrence from happening again or infecting other systems.

8. The IT Specialist will restore the affected system(s) to the uninfected state. This process may include the following tasks:
    a) Re-install the affected system(s) from scratch and restore data from backups if necessary. Preserve evidence before doing this.
    b) Make users change passwords if passwords may have been discovered.
    c) Be sure the system has been hardened by turning off or uninstalling unused services.
    d) Be sure the system is fully patched.
    e) Be sure real time virus protection and intrusion detection is running.
    f) Be sure the system is logging the correct events and to the proper level.

9. Evidence Preservation—make copies of logs, email, and other communication. Keep lists of witnesses. Keep evidence as long as necessary to complete prosecution and beyond in case of an appeal.

10. Assess damage and cost—assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.

11. Review response and update policies—plan and take preventative steps so the intrusion can't happen again. Important considerations include:

    a) Consider whether an additional policy could have prevented the intrusion.

b) Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
c) Was the incident response appropriate? How could it be improved?
d) Was every appropriate party informed in a timely manner?
e) Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
f) Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
g) Have changes been made to prevent a new and similar infection?
h) Should any security policies be updated?

17. This criteria applies to all campuses

This policy is applied across all locations including TCAT McMinnville and TCAT Manchester.

Exhibit A

Tennessee College of Applied Technology
Computer Operation and Internet Access Policy and Guidelines

• Compliance with this computer usage policy is necessary to ensure maximum utilization and performance of each computer system as well as provide a sense of security and restful cooperation among the school community. Strict adherence to this policy will prevent costly damage or repair, downtime, and loss of computer privileges.
• No computer system can be used without prior approval of the supervising instructor or other school official.
• Because software is protected under copyright laws, no software can be copied without written authorization.
• No outside software can be loaded on school computers without written approval.
• Changes to a system's configuration or the inappropriate deleting or changing of computer settings is forbidden.
• Technical manuals may not be removed from the training area.
• Computers must not be moved or repositioned on tables.
• To prevent damage to any system, computer users should not eat or drink within five (5) feet of a computer system, or smoke or vape around computer equipment.

Specific policy for access to the Internet

• The system may not be used for personal or private matters.
• Creating, distributing, or accessing hate mail, pornographic or obscene materials, discriminatory, or harassing materials, is strictly forbidden.
• Anti-social behaviors, including spamming are forbidden.
• Creating, distributing, or accessing confidential material, including but not limited to, test files or student/personnel records are forbidden.
• IMPORTANT NOTE: Any person who violates this policy will be subject to appropriate disciplinary sanction, including dismissal and/or possible prosecution. (See TBR Policy 3:02:00:01 regarding Student Conduct and Disciplinary Sanctions)

Copyright and Digital Millennium Act

• Materials published by the Tennessee College of Applied Technology McMinnville are protected by the Digital Millennium Copyright Act. The DMCA also requires that the institution inform all computer and network users that downloading of copyrighted material is prohibited. In addition, Tennessee Code Annotated §49-7-1(c) specifies that the institution ensure that no copyrighted digital music or videos be downloaded using institutional resources. Any attempts to do so will result in appropriate actions.

Violations

• Violations of the policy will result in action by the appropriate institution office. Students who violate this policy will be referred to the Coordinator of Student Services for appropriate action. Employees who violate this policy may be subject to disciplinary measures imposed by their supervisor in conjunction with the institution's administration. Violations of local, state or federal laws regarding unlawful access or use may be referred to the appropriate law enforcement officials for investigation and/or prosecution.

Inspection of Electronic Records

• Electronic records sent, received, or stored on computers owned, leased, or administered by the Tennessee College of Applied Technology McMinnville are the property of the College and the Tennessee Board of Regents. As the property of Tennessee College of Applied Technology McMinnville and TBR, the content of such records, including electronic mail, are subject to inspection by Tennessee College of Applied Technology McMinnville personnel. Users should have no reasonable expectation of privacy in the use of these resources.

Copyright General Information

• Copyright is a form of protection provided by the laws of the United States (Title 17, U.S. Code) to creators of "original works of authorship" including literary, dramatic, musical, artistic, and other published and unpublished works, when "fixed in a tangible form of expression." Protections last for the term of the author's life plus 50 years after death. It is given to individual, group, or corporate authors and to "works for hire".

• It is illegal for anyone to violate any of the rights provided to the owner of a copyright. The Copyright Act (1976) contains provisions prescribing damages that can be assessed if infringements are committed. In civil cases, the law allows the assessment of actual damages or statutory damages. For each infringement, statutory damages range from $250 to $10,000. These rights, however, are limited in scope. Sections 107-118 of the Copyright Act establish limitations that in some cases are specified as exemptions from liability. One major limitation is the doctrine of "fair-use" which is given statutory basis in Section 107 of the Act.

Acknowledgement

I have been instructed in computer and internet usage and understand the policies of Tennessee College of Applied Technology McMinnville.

Print
Name_____Signature_____

Exhibit B

TCAT McMinnville Computer Incident Report Form

1. Contact Information for this Incident:

Name:

Address:

Office Phone: Cell: Fax:

2. Physical Location of Affected Computer/Network:

(including building number, room number, and inventory information, if available):

3. Date and Time of the Incident Occurred:

Date: Time:

4. Type of Incident (check all that apply):

□ Intrusion
□ Root Compromise
□ Denial of service
□ Website Defacement
□ Virus/ Malicious Code
□ User Account Compromise
□ System Misuse
□ Hoax
□ Social Engineering
□ Network Scanning/Probing
□ Technical Vulnerability
□ Other (Specify):

4a. If a Virus,

Provide the name(s) of the virus(s):

Provide any URL with information specific to the virus:

Provide a synopsis of the incident:

Actions taken to disinfect and prevent further infection:

4b. If a Technical Vulnerability,

Describe the nature and effect of the vulnerability in general times:

Describe the conditions under which the vulnerability occurred:

Describe the specific impact of the weakness or design deficiency:

Indicate whether or not the applicable vendor has been notified:

5. Information on Affected System:

IP Address: Computer/Host Name: Operation System: (incl. release number) Other

6. How Many Host(s) are Affected:

□ 1 to 100 □ 100 to 1,000 □ More than 1,000

Signature_____S#_____Date_____

Exhibit C

Change Request Form

Change Request Information

Change Description		**Change title**	
Initiated by		**Priority (L,M,H)**	
Date		**Change number**	

Change Request Details

Description

Justification

Impact

Cost	
Schedule	
Resources	
Requestor	

Management Approval

Approval date		**Name**		**Decision**	☐ Accepted ☐ Rejected

Comments	