

Policy Name:
Effective Date:
Date of Last Revision:
Functional Area:

Information Technology. Policy and
Procedure Plan
04/06/2014
09/27/ 2022
Information Technology

Information Technology Policies And Procedures Plan

Tennessee College of Applied Technology Nashville
100 White Bridge Road
Nashville, TN 37209
Phone (615)-425-5575
Fax (615)-425-5581
www.tcatnashville.edu

Table of Contents

Introduction - Page 3

Scope – Page 3

Policy – Page 3

IT Staff /Stake Holders– Page 3

Description of IT Environment / Major Activities – Page 4

IT / Tech Access Budget – Exhibit C

Information Technology Policies Reviews and Revisions – Pages 21-22

TCAT-Nashville Computer and Network Policies

1. Acceptable Computer Use Policy
2. Copyright and Digital Millennium Act
3. Hardware/Software Change Control
4. Patch Management
5. Logging and Monitoring
6. User Access Control
7. User Access
8. Email Access
9. Disaster Recovery
10. Laptop Computer Security/Usage
11. Desktop Computer Security/Usage
12. Server Security/Usage
13. Server Audit Policy
14. Network Remote Access and VPN
15. Wireless Access
16. Computer Incidence Response
- 17 Criteria applies across all campuses

Exhibits

- A. Computer Operation and Internet Access Policy and Guidelines Form
- B. Computer Incident Report Form
- C. IT Budget

Yearly Policy Evaluation and Revision Members Pages 26-27

Introduction

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

Scope of Services:

TCAT-Nashville and its affiliated campuses IT Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the college which should be followed by all staff/faculty. It also provides guidelines TCAT-Nashville will use to administer these policies, with the correct procedure to follow.

Policy:

TCAT-Nashville 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 Coordinator's office and is located on the TCAT Voice Intranet page. These policies and procedures apply to all TCAT-Nashville and satellite campus employees.

IT Staff and Instructors

Terry Doss
(Work) 615-425-5575
(Work Cell) 615-630-4617
IT Coordinator reports to the President of TCAT-Nashville

Computer Information Technology Instructor – Nashville
Brad Marbach
Reports to the IT Coordinator of TCAT-Nashville
(Work) 615-425-5526
(Work Cell) 615-602-1589

Computer Information Technology Instructor - Portland
Joe Redemske
(Office) 615 395-5368
Reports to the IT Coordinator of TCAT-Nashville

IT Technician
Houston McPherson
(Work Cell) 615-630-4649
Reports to the IT Coordinator of TCAT-Nashville

Description of IT Environment

Network Setup – Infrastructure

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

Nashville Campus

- a. 1 g Windstream Fiber Internet Provided through AT&T
- b. 1 g Windstream Fiber Internet Provided through Comcast
- c. Fortinet 201F Firewall
- d. 28 Dell Managed Switches 48 Port
- e. 54 Enterasys Wi-Fi access points
- f. 20 g fiber connecting all switches
- g. 12 APC 1500 KVM battery backups

Portland Campus

- a. 500 m Windstream Internet Provided through Comcast
- b. Fortinet 101E Firewall
- c. 8 Dell Managed Switches 48 Port
- d. 17 Enterasys Wi-Fi access points
- e. 20 g fiber connecting all switches
- f. 3 APC 1500 KVM battery backups

Cockrill Bend Campus

- a. 100 m Windstream Internet Provided through Comcast
- b. Fortinet 101E Firewall
- c. 2 Dell Managed Switches 48 Port
- d. 8 Enterasys Wi-Fi access points
- e. 20 g fiber connecting all switches
- f. 2 APC 1500 KVM battery backups

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 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 is 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 Nashville 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 Nashville are the property of the College and the Tennessee Board of Regents. As the property of Tennessee College of Applied Technology Nashville and Tennessee Board Of Regents, the content of such records, including electronic mail, are subject to inspection by TTCN 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 D**).

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. SIMS 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-Nashville 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-Nashville 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-Nashville's information resources or systems and the associated access privileges. This policy applies at all times and should be adhered to whenever accessing TCAT-Nashville'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-Nashville'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-Nashville, 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-Nashville'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-Nashville owned PC's connected to the TCAT-Nashville'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 Coordinator before connecting any equipment to the TCAT-Nashville's network.

Operating System Access Control

Access to operating systems are controlled by a secure login process. The access control defined in the User Access Management section and the Password section above must be applied. The login procedure must also be protected by:

- a. Limiting the number of unsuccessful attempts, (5), and locking the account if exceeded. 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 complex characters as follows:
 - a. Use at least 1 character from 3 of the 4 following categories: Upper case, Lower case, Numbers (0-9), Symbols.
 - b. The following are acceptable symbols: @ # \$ % ^ - ! + = [] { } | \ : ' , . ? / ` ~ “ () ; < > or a blank space
- c. Cannot use one of your last 24 passwords
- d. Number requirement, lower case, symbol, blank spaces, 3 out of the 4 categories and at least 16 characters long). It is of utmost importance that the password remains protected at all times a. Never reveal your passwords to anyone.
- g. Never use the 'remember password' function.
- h. Never write your passwords down or store them where they are open to theft.
- i. Never store your passwords in a computer system without encryption.
- j. Do not use any part of your username within the password.
- k. Do not use the same password to access different TCAT-Nashville systems.
- l. 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 thru 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-Nashville IT Coordinator.

System Administration Standards

The password administration process for individual TCAT-Nashville systems is well-documented and available to designated individuals.

All TCAT-Nashville 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 Coordinator 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-Nashville'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 Coordinator.

7. User Access

Access to information must be specifically authorized in accordance with TCAT-Nashville'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-Nashville 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-Nashville. Access for contractors, consultants, or vendor personnel to TCAT-Nashville critical business information assets will be provided only on the basis of a contractual agreement.

8. Email Usage

Prohibited Use

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

Personal Use

Using a reasonable amount of TCAT-Nashville 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-Nashville email account is prohibited. Mass mailings from the TCAT-Nashville email system shall be approved by TCAT-Nashville Administration before sending. These restrictions also apply to the forwarding of mail received by a TCAT-Nashville employee.

Monitoring

TCAT-Nashville 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 PC and laptops, all user data is backed in the cloud thru One Drive. All hard drives are required to be encrypted thru Azure Active Directory Policy managed by TBR IT

Staff. The login is 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 location and is protect by S# or Portal Login with Multifactor Authentication. All campuses use the same guidelines using Azure Active Directory and One Drive. .In the event a PC's or laptop's are damaged the users will be given new devices and if internet access is restored or they are at another site they would sign in with student S# or (Portal ID) and secure multifactor authentication password. Devices will be restored from One Drive 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:

1. Restore critical applications to the most current date available. Updating the systems and databases will take place as the recovery effort progresses.
2. 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-Nashville site after repairs have

10. Laptop Computer Security/Usage

Appropriate measures should be taken when using laptops 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 laptops in order to protect TCAT-Nashville's capital assets. All data stored on desktop and laptop pc's must be stored in the Tennessee Board of Regents folder that is synced to Microsoft One dDrive

Laptops include: laptops, Smartphones, tablets, and authorized home laptops accessing the TCAT-Nashville network. The same general guidelines for desktop computers apply to TCAT-Nashville's laptops.

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

11. Desktop Computer Security/Usage

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

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

12. Server Security/Usage

General Configuration Guidelines:

1. Operating System configuration should be in accordance with approved SANS, (Sys Admin, Audit, Networking, and Security) Institute guidelines listed below.
 - a. 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-Nashville are configured according to the TCAT-Nashville security policies. Servers deployed at TCAT-Nashville shall be audited at least semi-annually using the Server Audit Hardening Checklist (**Exhibit F**) and as prescribed by applicable regulatory compliance

Audits may be conducted to:

1. Ensure integrity, confidentiality and availability of information and resources
2. Ensure conformance to TCAT-Nashville security policies

Guidelines:

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

1. All system logs shall be reviewed on a regular basis
2. All Administrator actions should be logged
3. Windows Updates should be downloaded and applied
4. Authentication restrictions for login
5. Password Complexity Restrictions to deter unauthorized access
6. All File Sharing permissions checked
7. Host security agent such as antivirus must be installed and updated
8. Verify the presence of Anti-Malware
9. Network scan to verify only required network ports and network shares are in use, PEN Test.
10. Verify administrative group memberships

14. Network Remote Access and VPN

Remote Access:

It is the policy of TCAT-Nashville that mobile computing and storage devices containing or accessing the information resources at TCAT-Nashville must be approved prior to connecting to the information systems at TCAT-Nashville. This pertains to all devices connecting to the network at TCAT-Nashville, 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-Nashville owned, that may connect to or access the information systems at TCAT-Nashville. A risk analysis for each new media type should be conducted and documented prior to its use or connection to the network at TCAT-Nashville 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-Nashville 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-Nashville, 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-Nashville employees may utilize the benefits of VPNs. Azure VPN access is managed and monitored by TBR IT.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to TBR secure networks
2. VPN access is accessed thru Microsoft Azure.
3. 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.
4. Users of computers that are not TCAT-Nashville owned equipment must configure the equipment to comply with TBR VPN and Network policies.
5. Only TCAT-Nashville - approved VPN clients may be used. (Azure VPN)
6. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of TCAT-Nashville's network, and as such are subject to the same rules and regulations that apply to TCAT-Nashville-owned equipment, i.e., their machines must be configured to comply with TCAT-Nashville Security Policies.
7. 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-Nashville'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-Nashville's networks.

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected to any of TCAT-Nashville'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 Coordinator, 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 Coordinator at 615-425-5575. (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 Coordinator 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 Coordinator will call those designated on the list. (TCAT-Nashville IT Coordinator-Terry Doss 615-630-4617. The staff member will log the information received in the same format as the IT Coordinator 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 Coordinator 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 Coordinator will recommend changes to prevent the occurrence from happening again or infecting other systems.
- 8) The IT Coordinator will restore the affected system(s) to the uninfected state. They may do any or more of the following:
- 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.
 - 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 Nashville, Cockrill Bend and Portland.

Exhibit A

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 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 is 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 Nashville 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 Nashville are the property of the College and the Tennessee Board of Regents. As the property of Tennessee College of Applied Technology Nashville and TBR, the content of such records, including electronic mail, are subject to inspection by Tennessee College of Applied Technology Nashville 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.

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

Print

Name _____ Signature _____

Exhibit B

TCAT-Nashville Computer Incident Report Form

This form is based upon the FedCIRC Incident Report Form, which Federal Agencies and Departments are requested to use when reporting an incident

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 barcode information, if available):

3. Date and Time of the Incident Occurred:

Date:

Time:

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

- | | |
|--|---|
| <input type="checkbox"/> Intrusion | <input type="checkbox"/> Root Compromise |
| <input type="checkbox"/> Denial of service | <input type="checkbox"/> Web Site Defacement |
| <input type="checkbox"/> Virus/ Malicious Code | <input type="checkbox"/> User Account Compromise |
| <input type="checkbox"/> System Misuse | <input type="checkbox"/> Hoax |
| <input type="checkbox"/> Social Engineering | <input type="checkbox"/> Network Scanning/Probing |
| <input type="checkbox"/> Technical Vulnerability | <input type="checkbox"/> 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 Applications:

(include hardware/software, version or release numbers): Signature S# Date

6. How Many Host(s) are Affected:

☐ 1 to 100

☐ 100 to 1,000

☐ More than 1,000

Exhibit C:IT Budget

FZRJF07 TBR8: 1.0

RUN

DATE 06-MAY-2022

Form VII

TN College of Appl Tech Nashville

RUN TIME 11:26 AM

Unrestricted Detailed Budget Proposals - Current

Fund Expenditures

July Budget 2022-23

Actual	October	Estimated	July
2020-21	2021-22	2021-22	2022-23
Technology Foundations (200080)			
Salaries - Academic			
60,195	62,050	62,050	62,151
Employee Benefits			
23,328	20,300	20,300	26,000
Travel			
0	500	500	500
Operating Expenses			
2,717	5,000	5,000	5,000
<hr/>			
Total - Technology Foundations (200080):			
86,240	87,850	87,850	93,651
<hr/>			
Technology Access Fee (299997)			
Operating Expenses			
67,446	175,500	175,500	175,000
<hr/>			
Total - Technology Access Fee (299997):			
67,446	175,500	175,500	175,000
<hr/>			
Financial Administration (450000)			
Salaries - Administrative			
102,709	143,435	141,435	185,322
Salaries - Supporting			
44,151	44,151	1,300	80,075
Salaries - Professional			
70,027	75,177	74,177	75,379
Employee Benefits			
98,056	139,000	134,000	141,000
Operating Expenses			
24,674	0	0	0
<hr/>			
Total - Financial Administration (450000):			
375,541	401,763	393,763	403,001
<hr/>			

IT Policy was reviewed annually by each committee member and revised as necessary.

IT Policy Evaluation and Revision Committee 2022

Added new password criteria, local hard drive encryption and multifactor authentication
The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Willoughby – Maintenance Coordinator

Terry Doss – IT Coordinator

Brad Marbach – CIT Associate Instructor

Adam Wills – Master 2 CAD Instructor

Christina Heard – Cosmetology Instructor Portland

IT Policy Evaluation and Revision Committee 2021

Added One Drive requirement for all data stored on PC's or Laptops to be synced to One Drive.

The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Lenz – President

Mark Willoughby – Maintenance Coordinator

Terry Doss – IT Coordinator

Andrew Cutchins – CIT Instructor Portland

Adam Wills – Master 2 CAD Instructor Nashville

IT Policy Evaluation and Revision Committee 2020 No Revisions

The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Lenz – President

Mark Willoughby – Maintenance Coordinator

Terry Doss – IT Coordinator

Andrew Cutchins – CIT Associate Instructor Portland

Policy/Change Review Committee 2019 No Revisions

The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Lenz – President

Mark Willoughby – Maintenance Coordinator

Terry Doss – IT Coordinator

Andrew Cutchins – CIT Associate Instructor Portland

IT Policy Evaluation and Revision Committee 2018

Removed all references to local server storage of Student Information. Needed because of change over to Banner.

The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Lenz – President

Mark Willoughby – Maintenance Coordinator
Terry Doss – IT Coordinator
Andrew Cutchins – CIT Associate Instructor Portland
David Burks – Tech Foundations Instructor Nashville/Portland

IT Policy Evaluation and Revision Committee 2017-No revisions

The following IT Review Committee members have evaluated the IT Security Policy annually and revised as necessary.

Mark Lenz – President
Mark Willoughby – Maintenance Coordinator
Terry Doss – IT Coordinator