TENNESSEE COLLEGE OF APPLIED TECHNOLOGY
DICKSON & CLARKSVILLE CAMPUS

Policy Name:	Information Security
TBR Policy Number:	N/A
TCAT-D Policy Number:	IT-105
Effective Date:	December 15, 2015
Date of Last Revision:	November 22, 2021
Date of Last Review:	October 6, 2021
Functional Area:	Information Technology

Information Security Plan

This Information Security Plan describes the plans of Tennessee College of Applied Technology Dickson (TCAT-Dickson) to safeguard and to protect covered data and information. These safeguards are provided to:

- Ensure the security and confidentially of covered data and information;
- Protect against anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of covered data and information that could result in substantial harm or inconvenience to any student or employee.

This Information Security Plan also provides for mechanisms to:

- Identify and assess the risks that may threaten covered data and information maintained by TCAT-Dickson;
- Develop written policies and procedures to manage and control these risks;
- Implement and review the plan; and
- Adjust this plan to reflect changes in technology, the sensitivity of covered data and information and internal or external threats to information security.

Identification and Assessment of Risks to Student Information

TCAT-Dickson recognizes that risks are both internal and external. These risks include, but are not limited to:

- Unauthorized access of covered data and information by someone other than the owner of the covered data and information;
- Compromised system security as a result of system access by an unauthorized person;
- Interception of data during transmission;
- Loss of data integrity;

- Physical loss of data in a disaster;
- Errors introduced into the system;
- Corruption of data or system;
- Unauthorized access of covered data and information by employees;
- Unauthorized request for covered data;
- Unauthorized access through hardcopy files or reports;
- Unauthorized transfer of covered data and information through third parties.

This list may not be a complete detailing of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly.

The TCAT-Dickson believes the current safeguards are reasonable and, in-light-of the on-going check, the current risk assessments are sufficient to provide security and confidentially to covered data and information by the College. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Information Security Plan Coordinator

The Information Technology (IT) Coordinator has been appointed as the administrator of this plan. The IT Coordinator is responsible for assessing the risks associated with unauthorized transfers of covered data and information and implementing procedures to minimize those risks to TCAT-Dickson.

Design and Implementation of Safeguards Program

Employee Management and Training

References of new employees working in areas that regularly work with covered data and information, such as Human Resources, Business Office, and Financial Aid are verified upon hiring. During the employee orientation, each new employee in these departments receives proper training on the importance of confidentially of student records, student financial information, and other types of covered data and information. Each new employee is also trained in the proper use of computer information and passwords. Training includes controls and procedures to prevent employees from providing confidential information to an unauthorized individual.

Each department responsible for maintaining covered data and information is tasked with taking the necessary steps to protect information from destruction, loss, or damage due to environmental hazards, such as fire and water damage or technical failures. Further, through the Vice-President's office, who serves as the Affirmative Action Officer, each department is responsible for maintaining covered data and information. The Affirmative Action Officer coordinates with the Office of General Counsel on an annual basis for the coordination and review of additional privacy training appropriate to each department.

All employees are trained on the importance of maintaining data safeguards. These training efforts help to minimize risk and safeguard covered data and information security.

Physical Security

TCAT-Dickson has addressed the physical security of Student Services Department covered data and information by;

- Limiting access to only those employees who have a business reason to know such information;
- Personal student information, accounts, balances and transactional information are available only to TCAT-Dickson employees with an appropriate business need for such information;
- Account information and other paper documents are kept in file cabinets, rooms, or vaults that are locked;
- Only authorized employees know lock combinations and the location of keys; and
- Paper documents that contain covered data and information are shredded or are placed in a locked bin at time of disposal and picked up by a State approved document disposal company.

Information Systems

Access to covered data and information via TCAT Dickson's computer information system is limited to those employees who have a business reason to know such information.

- Each employee is assigned a user name and password, which is changed on a regular basis in methods compliant to TBR policies and guidelines. Passwords must have a minimum of 8 characters with (1) capital letter, (1) special character, and (1) number; and

- Databases containing personal covered data and information, including but not limited to accounts, balances, and transactional information, are available only to TCAT Dickson employees in appropriate departments and positions.

TCAT-Dickson takes reasonable and appropriate steps consistent with current technological developments to make sure that all covered data and information is secure and to safeguard the integrity of records in storage and transmission;

- External access to the servers and all workstations is controlled by a hardware firewall. Internal access is controlled by server and workstation accounts, access rights, and passwords.
- Instructors maintain their employee computers, as well as classroom and lab computers, with monthly maintenance by updating the operating system and applications; running appropriate cache cleaners, CCleaner for example, and defragmenting the computer; ensuring that virus software is in place; and, approving appropriate patches and updates in a timely fashion. Instructors are responsible to ask the IT Coordinator for guidance and/or assistance as needed. A monthly plan of maintenance tasks are provided in Attachment A.
- User and system passwords are also required to comply with TCAT-Dickson's Password Policy;
- In addition, an intrusion detection system has been implemented to detect and stop certain internal threats along with an Incident Response Policy for occasions where intrusions do occur.

When commercially reasonable, encryption technology will be utilized for both storage and transmission.

- All covered data and information will be maintained on servers that are behind TCAT-Dickson's firewall;
- All firewalls software and hardware are maintained and kept current;
- There is a written IT plan which contains a number of policies and procedures to provide security to TCAT-Dickson's information systems;
- These policies are available to all employees through the Tennessee Board of Regents website at www.tbr.edu;

- Paper copies are available upon request.

Social Security Numbers

The release of personal social security numbers is prohibited in any form.

Selection of Appropriate Service Providers

Due to the specialized expertise needed to design, implement, and service new technologies, vendors may be needed to provide resources that TCAT-Dickson determines not to provide on its own. In the process of choosing a service provider that will maintain or regularly access covered data and information, the evaluation process shall include the ability of the service provider to safeguard confidential financial information. Contracts with service providers may include the following provisions:

- An explicit acknowledgement that the contract allows the contract partner access to confidential information; And, they may be thoroughly vetted by the Tennessee board of Regents (TBR) in its contracts procedures.
- A specific definition or description of the confidential information being provided;
- A stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- An assurance from the contract partner that the partner will protect the confidential information it receives according to commercially acceptable standards and no less rigorously than it protects its own confidential information.
- A provision providing for the return or destruction of all confidential information received by the contract provider upon completion or termination of the contract;
- An agreement that any violation of the contract's confidentiality conditions may constitute a material breach of the contract and entitles TCAT-Dickson to terminate the contract without penalty; and
- A provision ensuring that the contract's confidentially requirements shall survive any termination agreement.

Continuing Evaluation and Adjustment

This Information Security Plan will be subject to periodic reviews and adjustments. Continued administration of the development, implementation, and maintenance of the program will be the responsibility of the designated IT Coordinator who will assign specific responsibilities for the upkeep of all information of covered data. The IT Coordinator, in consultation with the President, will review the standards set forth in this policy and recommend updates and revisions as necessary. It may be necessary to adjust the plan to reflect changes in technology, the sensitivity of the covered data, and internal or external threats to information security.

Any complaints and possible violations of this plan should be reported to the IT Coordinator or the President.

This plan shall encompass the rules on Family Education Rights and Privacy Act (FERPA) of 1974, Federal Trade Commission (FTC), Tennessee Board of Regent Guideline B-090, Subject: Safeguarding of Customers' Nonpublic Financial Information (Gramm-Leach-Bliley Act), and Guideline S-02, Subject: Confidentially of Student Records.

*Covered data and information – Student personnel file, employee personnel file, budget information with employee data, etc.

Attachment A

Monthly Employee and Classroom/Lab Computer Maintenance Tasks

Each instructor and staff member is responsible for completing regular maintenance on each computer within their office and classroom/lab.

Maintenance Plan for Windows Systems;

The programs listed below that will remove the unused cache files that slow your system down and could possibly contain viruses and/or spyware.

a. CCleaner – run each time the computer system reboots;

1. Complete all updates. Click --> Start ... Windows update. Once all updates are installed, move to the next step.

    a. Click and run CCleaner. There are several tools in this program so be sure to run these two: (*note: you can use the Tools option there to uninstall any programs on your systems you want removed.)*