Policy No: G009 – Media Services Plan

EFFECTIVE DATE: July 2005
Revised: June 2022, January 2021, November 2016, July 2013, December 2011, July 2009

This plan will focus on specific items to ensure that proper reviewing, revising, reporting and implementation of the following areas:

- Media Services
- Educational Material
- Educational Equipment

Plan Objectives

To assure that media resources are readily available to students, staff and faculty members.

The Scope and Availability

The media services available to the campus community are current and relevant educational material to help fulfill the needs of the educational programs. A listing of media resources can be found on the College's library system (ResourceMate), this system can be accessed at the front desk and through any internet connection. Media Services include the Library, Computer Laboratory and educational equipment.

The College provides access to students and faculty members to online reference material, by combining multiple online databases into one large database with one easy-to-use access point, students and faculty members have access to the Library and Information Resources Network (LIRN) and Florida Electronic Library including: Gale InfoTrac, ProQuest, CREDO reference, elibrary, Bowker and EBSCO all adding up to over 132 million journal articles, documents, books, encyclopedias, newspapers, magazines, video and audio files. These resources are available 24 hours a day, seven days a week from any computer on the campus or any computer with Internet access. Remote access to online reference material can be reached from http://www.taylorcollege.edu/library/. If accessing remotely, users will be asked for a password, this information is given out by the Program Director, Faculty and Librarian.

Hours of Availability

Library	9:00 am to 5:30 pm Monday – Friday
Computer Laboratory	9:00 am to 5:30 pm Monday – Friday

Responsible Staff Member(s)

The Senior Director of Finance and Operations, Librarian and IT Support (Think Technologies) are responsible for implementation and coordination of media services. Roles and responsibility include the following:

- Purchase of additional media services and supplies.
- Ensure organization of available media services.

- Ensuring that online resources and system hardware is working correctly.
- Compiling the results for the annual review of the plan
- Maintain Equipment Listing (identify whether Instructional or Non-Instructional and include location, number of items, date of purchase and purchase price and/or current value)

Orientation

Taylor College has an orientation to all new users at the beginning of a program or employment.

Facilities

Facilities used for media services include the Library and Computer Laboratory.

Budget

The college's annual budget allocates funds to the repair and purchase new media supplies, equipment and additions to the media services.

Evaluation, Review and Revision

The Media Services plan is evaluated by program completers at the end of a program and by staff and faculty annually. During the Institutional Assessment meeting, all completed evaluations are reviewed to evaluate the effectiveness of media services provided by the college and the utilization of the results to modify and improve media services.

Policy No: G010 – Security Policy & Procedure for all Media

EFFECTIVE DATE: June 2020
Revised: June 2022

APPLICABILITY/ACCOUNTABILITY

This policy applies to all employees of Taylor College who maintain or use college data. This includes all full-time and part-time employees, adjuncts, and others on temporary or time-limited appointments, and all persons paid by or through the college such as contractors, consultants, or employees of direct support organizations.

INCIDENCE RESPONSE POLICY

Data are critical assets of Taylor College. All members of the college community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the college regardless of the medium on which the data resides, such as electronic, paper, or other physical form, or how the data may be transmitted such as email, text message, facsimile or other means. It is the policy of Taylor College to classify types of data in use at the college and to provide the appropriate levels of information security and protection for all personally identifiable information.

Individuals working for or on behalf of Taylor College who create, view, or manage college data are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, storage of, and disposal of college data in compliance with this policy. The President must be notified immediately if data classified as highly restricted or restricted is, or is suspected to have been, lost or disclosed to unauthorized parties, or if any unauthorized use of Taylor College's information systems is occurring or is suspected to have occurred. State and Federal laws require that unauthorized access to certain restricted information must be reported to the appropriate agency or agencies. In the event there is a breach of Taylor College's network, as a precaution a notice, Security Incidence Response form will be completed and sent as directed on the form. In the event of a suspected information security incident, users should take no action to delete any data or attempt to investigate. Taylor College's Director of Compliance and Local Agency Security Officer, LASO, will contact the Information Security Officer, ISO, at the Florida Department of Law Enforcement, FDLE.

Personally Identifiable **Information** PII POLICY

Taylor College is committed to protecting all Personally Identifiable Information against any inappropriate access and use in compliance with applicable laws and regulation. Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, or removal of inappropriate information posted on Taylor College's owned computers or the college's supported Internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination.

DATA RESTRICTIONS

Restricted

Sharing of Restricted information within the College may be permissible if necessary to meet Taylor College's legitimate business needs. Except as otherwise required by law (or for purposes of sharing between law enforcement entities), no Restricted information may be disclosed to parties outside Taylor College, including contractors, without the proposed recipient's prior written agreement (i) to take appropriate measures to safeguard the confidentiality of the Restricted information; (ii) not to disclose the Restricted information to any other party for any purpose absent the University's prior written consent or a valid court order or subpoena; and (iii) to notify Taylor College in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of restricted information within Taylor College must comply with Taylor College policies.

Examples of restricted data include business-sensitive data, proprietary intellectual property data, and student academic records as defined by the Family Educational Rights and Privacy Act (FERPA) of 1974, and other data protected by law or regulation.

The following College Information is classified as Restricted:

- Social security number
- Bank account number
- Driver's license number
- State identity card number
- Credit card number
- Protected health information (as defined by HIPAA)

Criminal Justice Information Services, Florida Department of Law Enforcement, FDLE, background checks are considered restricted data that are confidential and may contain critical information.

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of Taylor College. Taylor College shall adhere, at a minimum, to the CJIS Security Policy. While Taylor College may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

Procedure for Information Handling Policy/Media Protection/Physical Protection

- Background check notification is emailed to the Campus Registrar or Campus President from FLDE
- The authorized employees will log into the FLDE site to review the backgrounds to determine which are employees and which are student backgrounds
- The college registrar prints out all background for employees and given to the executive assistant to file in the employees Human Resource file and is placed in a locked cabinet located in the President's office.

- The Campus Registrar prints out all backgrounds for students and employees. The Admissions Department is notified by the Registrar if the student is either cleared or not cleared to further the Admissions Application. At no time will the background report be handled by unauthorized personnel.
- Registrar files background check copies into a separate file which is placed in a locked cabinet and the cabinet is in the TC file room, that has a secured locked door
- Only employees that have completed the Security Awareness Training Level 4 are allowed to transport or file the CJI.
- Any files that have been scanned that contain CJI are held on an external hard drive that is encrypted. The external hard drive is stored in a cabinet in the limited access records room. Authorized personnel to the records room, are the President, registrar, Financial Aid Director, Financial Aid Staff. Only Campus President, Campus Registrar, and Compliance Director are allowed access to the CJI files.
- After one year, background checks are destroyed. A certified shredding company will remove this material from the locked shred-it box under the supervision of a TC employee.

Confidential Information Exchange Policy

Taylor College Information is classified as Confidential if it falls outside the restricted classification, but is not intended to be shared freely within or outside Taylor College due to its sensitive nature and/or contractual or legal obligations. Examples of Confidential Information include all non-Restricted information contained in personnel files, misconduct and law enforcement investigation records, internal financial data, donor records, and education records (as defined by FERPA).

Sharing of Confidential information may be permissible if necessary to meet the Taylor College's legitimate business needs. Unless disclosure is required by law (or for purposes of sharing between law enforcement entities), when disclosing Confidential information to parties outside Taylor College, the proposed recipient must agree (i) to take appropriate measures to safeguard the confidentiality of the information:(ii) not to disclose the information to any other party for any purpose absent Taylor College's prior written consent or a valid court order or subpoena; and (iii) to notify Taylor College in advance of any disclosure pursuant to a court order or subpoena unless the order or subpoena explicitly prohibits such notification. In addition, the proposed recipient must abide by the requirements of this policy. Any sharing of confidential information within Taylor College must comply with Taylor College policies.

Disposal of Data Restricted Files and Document Destruction

The CJI is stamped "DO NOT SCAN" Non-enrolled student files remain in the secure file room, that has a secured locked door and are scheduled for disposal after one year if the enrollee does not become an enrolled student. The file contents including the CJ, is placed in a secured locked bin designated for shredding.

Once a student's cohort has graduated, The CJI is removed from the academic file and placed in the secured locked bin for shredding. The other contents of the academic file are scanned and uploaded to the computer system and stored on a secured server with limited access. After it has been verified the file has been scanned it its entirety the file contents are placed in the secured locked bin designated for shredding.

Student financial aid files are scheduled for disposal after three years and follow the same procedure as the academic file for shredding.

DISPOSAL OF PHYSICAL MEDIA POLICY

When the shredding company arrives a Taylor College employee escorts the shredder company employee to pick up the secured shredder bins, then the Taylor College employee with the shredding company employee goes to the shredding machine located inside the back of a truck and observes the shredding of the entire container(s).

Personally Owned Devices

Personally owned devices include cell phones, tablets or any other device that is owned and maintained by the user, not Taylor College.

The overriding goal of this policy is to comply with the CJIS Security Policy requirements. Due to the evolving nature of the CJIS Security Policy, it is necessary to separately communicate the requirements of the CJIS Security Policy as they are developed and enhanced. These additional requirements are intended to be an enhancement to the existing Standard Operating Procedures of Taylor College. Taylor College shall adhere, at a minimum, to the CJIS Security Policy. While the Agency may augment or increase the standards, it cannot detract from the minimum requirements set forth by the FBI CJIS Security Policy.

This pertains to all Taylor College employees. Taylor College does not allow personally owned devices to access, store or transmit criminal justice information. Under no circumstance are users allowed to connect their personal device to Taylor College's network or any Taylor College owned devices, applications or systems.

POLICY VIOLATION: Any user who violates any portion of this policy will be subject to the standard disciplinary processes in place with Taylor College. Sanctions against staff that violate information systems and or security policies may include formal disciplinary action up to and including termination based on offense severity.

COMPUTER SECURITY

Taylor College provides access to computers, the internet, and information resources to the student body, faculty, and staff. Most of Taylor College's financial, administrative, and, academic systems are accessible through the institution's managed network.

At Taylor College security is critical to the physical network, computer operating systems, and the administrative programs.

Confidentiality, privacy, access, accountability, authentication, and network maintenance are components of a comprehensive security plan. This plan identifies key concerns and an issue faced by Taylor College at the application, host and network level, and strives for a balance between Taylor College's desire to promote and enhance the free exchange of ideas and its need for security of critical information and systems.

This document assists in identifying and defining the following:

1. Identify the elements of a good security policy;
2. Explain the need for Information Technology security;
3. Specify the various categories of Information Technology security;
4. Indicate the Information Technology Security responsibilities and roles; and
5. Identify appropriate levels of security through standards and guidelines.

This document establishes Taylor College's security policy, establishes standards, guidelines and operating procedures while addressing student and staff specific and individual needs.

Elements of a good security policy include:

- Confidentiality and Privacy
- Access Control Requirements
- Accountability
- Authentication Strategy and Management
- Availability
- Information technology system and network maintenance policy

Confidentiality*:* refers to the Taylor College needs, obligations and desires to protect private, proprietary and other sensitive information from those who do not have the right and need to obtain it.
Access Control Requirement**:** defines rights, privileges and mechanisms to protect assets from access or loss.
Accountability**:** defines the responsibilities of users, operations staff and management.
Authentication Strategy and Management**:** establishes password authentication policy and procedures for distribution and controls.
Availability*:* establishes hours of resource availability, redundancy and recovery, and maintenance downtime periods.
Information technology system and network maintenance**:** describes how both internal and external maintenance people are allowed to handle and access technology.

Need for Information Technology Security

Taylor College and all members of the institution are obligated to respect and, in many cases, to protect **confidential** data. Academic records, student records, certain employment-related records, and progress communications are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including faculty and other personnel records, and records relating to the institution's business and finances are, as a matter of institutional policy, treated as confidential.

Taylor College recognizes that it has both internal and external risks. 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 systems
- Unauthorized access of covered data and information by employees
- Unauthorized requests for covered data and information
- Unauthorized access through hardcopy files or reports
- Unauthorized transfer of covered data and information through third parties

Taylor College recognizes that this may not be a complete list of the risks associated with the protection of covered data and information. Since technology growth is not static, new risks are created regularly. Accordingly, the school works with information technology vendors to actively monitor for identification of new risks. The school believes its current safeguards are reasonable and, in light of the school's current risk assessments are sufficient to provide security and confidentiality to covered data and information maintained by the school. Additionally, these safeguards protect against currently anticipated threats or hazards to the integrity of such information.

Systems (hardware and software) designed primarily to store confidential records (such as the Financial Information System and Student Information System) require enhanced security protections and are controlled ***(strategic)*** systems to which ***access*** is closely monitored. Networks provide connection to records, information and other networks and also require security protections. The use of Taylor College Information Technology assets in other than a manner and for the purpose of which they were intended represents a misallocation of resources and, possibly, a violation of law.

This policy applies to the following categories of security:

- ***Computer system and applications security****:* Central processing unit, peripherals, operating system and data
- ***Physical security***: The premises occupied by the Information Technology personnel and equipment
- ***Operational security***: Environment control, power equipment, operational activities
- ***Procedural security***: Established and documented security processes for information technology staff, vendors, management and individual users
- ***Network security****:* Communications equipment, personnel, and cable areas

Responsibility and Roles for Appropriate Security

Data, systems and networks are assigned to Taylor College management, directors and department heads. In many cases, responsibility for designing, implementing and maintaining security protections will be delegated to information technology support personnel, but the director or department head will retain responsibility for ensuring compliance with this policy. In addition to management and information technology support staff, the individual user is responsible for the information technology equipment and resources under his or her control.

At Taylor College, the President and IT department is responsible for:

- Tracking technology and regulatory changes that may indicate or require a change or addition to the current policy;
- Advising affected campus and department management and staff of said changes;
- Establishing protocols that support the implementation and maintenance of the security policy;

- Lead department and campus needs to develop, implement and maintain their understanding of the security policies that support and facilitate the institution; and
- Establishing and maintaining a repository for Taylor College's collected security documents.

Security Provisions

The Taylor College Information Security Plan herein is designed to ensure the security, integrity, and confidentiality of covered data, including but not limited to non-public personally identifiable information, protecting it against anticipated threats, and guarding it against unauthorized access or use. Covered under the Plan are administrative, technical, and physical safeguards used in the collection, distribution, processing, protection, storage, use, transmission, handling, or disposal of covered data. The Plan covers actions by both employees of the school and outside service providers.

The school uses direct personal control or direct supervision to control access to and handling of all covered data when an office is open. Whether the information is stored in paper form or any electronically accessible format, covered data is maintained, stored, transmitted and otherwise handled under the direct personal control of an authorized employee of the school.

Covered data is collected, processed, transmitted, distributed and ultimately disposed of with constant attention to its privacy and security. Conversations concerning covered data are held in private. Papers with covered data are mailed via official campus mail, US mail, or private mail carrier. When best practices permit the disposal of non-public information, it is destroyed; paper containing such information is routinely shredded or otherwise destroyed.

School employees are required to password-protect electronic files of non-public personally identifiable information when transmitting electronically.

Confidential material is kept secure. Most offices have locked doors with restricted access. For those that do not, materials are kept in locked filing cabinets or other locked storage areas. When offices are open, confidential information is kept out of sight from visitors, and computer screens are not visible to visitors. Offices and/or computers are locked when the office will be vacant for an extended length of time.

Key access is limited to authorized school employees only, in the context of school key control governing the distribution of keys. The President further ensures the security of offices after hours.

Confidentiality & Privacy

Taylor College and all members of the institution are obligated to respect and, in many cases, to protect confidential data. There are, however, technical and legal limitations on our ability to protect confidentiality.

For legal purposes, electronic communications are no different than paper documents. Electronic communications are, however, more likely to leave a trail of inadvertent copies and more likely to be seen in the course of routine maintenance of computer systems. Certain areas of the institution permit incidental personal use of computer resources. Taylor College does not monitor the content of personal Web pages, email or other online communications. However, Taylor College must reserve the right to examine computer records or monitor activities of individual computer users:

a) To protect the integrity or security of the computing resources or protect Taylor College from liability,
b) To investigate unusual or excessive activity,
c) To investigate apparent violations of law or university policy, and
d) As otherwise required by law or exigent circumstances.

In limited circumstances, Taylor College may be legally compelled to disclose information relating to business or personal use of the computer network to governmental authorities or, in the context of litigation, and/or to other third parties. Administrators of Taylor College, campuses, or staff should notify computer users if incidental personal use is not permitted and that the Taylor College cannot ensure the confidentiality of personal communications.

Access

No one may access confidential electronic records unless specifically authorized to do so. Student Financial Aid access requires additional levels of security and screening, therefore, this restricted access is by approval and must be met with additional measures of confidentiality. Even authorized individuals may use confidential records only for authorized purposes. Taylor College requires that all students, faculty, administration, and leadership of the institution respect the privacy of others and their accounts, not access or intercept files or data of others without permission, and not use another person's password or access files under false identity. Violators of any of these rules are subject to discipline consistent with the general disciplinary provisions applicable to faculty, staff or students.

Technology assets are to be housed in an appropriately secure physical location. Technology assets include servers, personal computers that house systems with controlled access (laptops are a category of special consideration), ports (active ports in public areas), modems and network components (cabling, electronics, etc.).

Passwords help protect against misuse by seeking to restrict use of school systems and networks to authorized users. Each authorized user (specific individual) is assigned a unique password that is to be protected by that individual and not shared with others, is difficult to crack, is changed on a regular basis, and is deleted when no longer authorized.

<u>Passwords must be</u>:

- Changed by the user on-line every ninety days
- Eight characters in length, minimum
- At least one capital letter
- At least one lowercase letter
- At least on number
- Significantly different from prior passwords
- Recommend using a special character for example &@*! Special characters are not required but do increase the security
- Individuals are expected to protect passwords from disclosure. Every individual must have their own user login

Password level authentication is required by any users that access company data, secondary authentication method is required for any user accessing student records including the Student

Information System. All new users are given a temporary authenticator that is issued by the network administrator and will never be emailed or delivered electronically. If a password is forgotten, lost or believed to have been compromised the use will immediately contact their supervisor or the network administrator. The network administrator will then issue a new temporary password. The old password will be reset as will the password of a user that leaves the company for any reason.

The management will ensure that controls are in place to avoid unauthorized intrusion of systems and networks and to detect efforts at such intrusion. Such controls may include some combination of the following: internet traffic monitoring; monitoring successful and unsuccessful access to data; and conducting port scans to ensure that only authorized users are connected to the network.

Accountability

Individual users are responsible for ensuring that other users do not access the system data with another user log in privileges. In particular, users must take great care in protecting their usernames and passwords from eavesdropping or careless misplacement. Passwords are never to be 'loaned.' Individual users will be held responsible for any security violations associated with their usernames. Operations staff is responsible for reviewing the audit logs and identifying potential security violations. The operations staff is responsible for establishing the security and access control mechanisms (such as usernames, passwords, logging, etc.) and may be held accountable for any security breaches that arise from improper configuration of these mechanisms

Additionally, as users are granted access to controlled internal and external systems, they will receive written statements (specific to the individual application and authored by the security administrator for that application) outlining the user's responsibility regarding the appropriate use of the system and data and emphasizing the consequences of improper use. This statement is to be read and signed by each user.

Each user permitted to access a controlled system is to be made aware of the access policy for that system. Management will provide this information to the employee when first granting access and make the employee aware of the auditing capability in place to verify compliance.

Downloading software, particularly software that is not job-related or endorsed by the administration, may introduce security risks and will not be allowed unless authorized in accordance with the procedures set forth herein.

RIGHTS AND RESPONSIBILITIES

Computers and networks provide access to resources on and off the campus location, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

Students and employees may have rights of access to information about themselves contained in computer files, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files as required, to protect the integrity of computer systems. For example, following organizational guidelines, system administrators may

access or examine files or accounts that are suspected of unauthorized use or misuse, or that have been corrupted or damaged.

Outside Service Providers

Third party service providers are required to maintain appropriate safeguards for nonpublic information to which they have access. Contracts with service providers, who within their contracts have access to Taylor College non-public student, prospective student, employee and/or customer information, shall include the following provisions as appropriate:

- Explicit acknowledgment that the contract allows the contract partner access to confidential information;
- Specific definition of the confidential information being provided;
- Stipulation that the confidential information will be held in strict confidence and accessed only for the explicit business purpose of the contract;
- Guarantee from the contract partner that it will ensure compliance with the protective conditions outlined in the contract;
- Guarantee from the contract partner that it will protect the confidential information it accesses according to commercially acceptable standards and no less rigorously than it protects its own customers' confidential information.
- Provision allowing for the return or destruction of all confidential information received by the contract partner upon completion of the contract.
- Stipulation that any violation of the contract's protective conditions amounts to a material breach of contract and entitles Taylor College to immediately terminate the contract without penalty.
- Provision allowing auditing of the contract partners' compliance with the contract safeguard requirements.
- Provision ensuring that the contract's protective requirements shall survive any termination agreement.

If the school has entered into an arrangement with an outside servicer provider, note that Federal regulation 34 CFR §668.25, includes a provision that the school remains liable for any action by its third-party servicers.

Media Protection, Sanitization and Disposal

All physical media including servers and onsite backup drives are protected by password level authentication. The server and backup drives are kept locked in a locked fire-proof room with limited key access. Login to the server directly will be strictly forbidden other than domain administrative level authentication. Backup drives are an image requiring a password which encrypts the data. Any data removed or recovered from a backup will be documented in the document named “data handling and recovery log”

All data is required to be sanitized using DoD5220.22-M Standards. All computer laptops and tablets used to access student or company data will be sanitized by the network admin or technician. The disposal will be documented and logged in the document named “data and devise destruction log”.

If a computer or backup drive needs to be destroyed the steps shall be documented in the log “data and device destruction log” the sanitized physical devises will be taken to a local company the recycles

the materials but does not refurbish or reuse.

Existing Legal Context

All existing laws (federal and state) and Taylor College institutional regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply generally to personal conduct. It is understood that according to the requirements of the Federal Student Aid User of Electronic Services Statement, our institution is held accountable for any and all actions taken with the SAIG enrollment process, and that the use of the electronic system operates on the premise that Destination Point Administrators (DPA) are the responsible parties for maintaining updated and current Federal Student Aid User of Electronic Services Statements for each person they grant access to FAA Access to CPS Online or EDconnect. The DPA determines the users who are allowed access to these electronic services. With the collection of the information on each staff person granted access in accordance to the Statement it is understood that each represents the institution and must have on file an active and current electronic services user document.

Specific to the access rights granted, there is a Zero Tolerance of any misuse of computing, networking, or information resources and any abuse of privilege which may result in the restriction of and or the termination of any/all computing privileges. Additionally, any misuse of student or institutional information can be prosecuted under applicable statutes related to student or institution data. Misuse and/or Abuse is defined and represented in reference to computer, network, and Internet security, where the terms “misuse” and "abuse" (known as IT-abuse or information abuse) describes willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources and/or email or other electronic accounts. Users are held accountable for their conduct under institution policies, procedures, or related servicing agreements.

Complaints alleging misuse of any computing and network resources will be directed to the office of the President who is responsible for taking appropriate disciplinary action. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment.

Federal Student Aid Security Policy

Student Aid access, NSLDS, COD, FSA, FAA, CPS awarding and reconciliation areas are considered to be function specific requirements and, therefore, persons not directly involved are prohibited by Taylor College from accessing these data bases or systems. Taylor College specifically identifies those employed persons with a vital need for system, as in the Financial Aid staff, and controlled access will be granted.

Student aid information contains data protected under the Privacy Act and therefore it is the position of the administration of Taylor College that it needs to be protected from unauthorized access. In light of the information shared within Student Aid, Taylor College expects and requires user security awareness and professional conduct for all persons designated as users.

Prior to being granted access to any secure Federal Student Aid system, the Taylor College Information Technology Specialist, who controls the access for all users, must review the computer use policy with the designated person. In addition, each new user is made aware of the potential risk to the Federal

Student Aid data within the system and is strongly advised that any such misuse will not be tolerated. Taylor College ensures that anyone who is granted access must be versed in the rules regarding access and use, and, that acceptable behavior is expected while being permitted to access the system. Taylor College states that effective security is an administrative effort involving the participation[s] that is/are granted user access designations and the Financial Aid Director, DPA/President who ensures that all persons are in compliance. It is further explained that it is the responsibility of each user to know and follow the appropriate guidelines.

Examples of Misuse of Computer(s)

COURSE OF ACTION FOR NSLDS SYSTEM USER VIOLATIONS:

Sharing a NSLDS User ID on the NSLDS is a *SERIOUS NSLDS SYSTEM USER VIOLATION.* This type of Violation/Sharing a NSLDS User ID on NSLDS may cause permanent User Revocation on the NSLDS System.

Examples of misuse include, but are not limited to, the activities in the following list:

- Using a computer account that you are not authorized to use.
- Obtaining a password for a computer account without consent.
- Using the Campus Network to gain unauthorized access to any computer systems.
- Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network.
    - This includes but is not limited to programs known as computer viruses, Trojan horses, and worms.
- Attempting to circumvent data protection schemes or uncover security loopholes.
- Violating terms of applicable software licensing agreements or copyright laws.
- Deliberately wasting computing resources.
- Using electronic mail to harass others.
- Masking the identity of an account or machine.
- Posting materials on electronic bulletin boards that violate the institution’s codes of conduct.
- Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Activities will not be considered misuse when authorized by appropriate Taylor College officials for security or performance testing as required to maintain the integrity of the information system and its components, portals, end user stations, and/or any student access points including wireless.

Appropriate Computer Use

Taylor College extends to students, faculty, and staff the privilege to use its computers and network. Taylor College provides access to the campus network and enables users, students, staff and administration to send and receive electronic mail messages, share in the exchange of ideas, and, to use Web browsers and other Internet tools to search and find needed information.

The Internet user community observes informal standards of conduct. All persons accessing the internet via any connection supported or otherwise originated through Taylor College is expected to understand that the appropriate, considerate behavior is expected in order to make using the Internet a positive, productive, experience throughout the education experience at Taylor College. All students, staff, and administrators are expected to comply with these informal standards and be a "good citizen" of the Internet.

Enforcement

Penalties may be imposed under one or more of the following: Policies covered under FERPA, Florida law, or the laws of the United States related to student information, data, or privacy. Minor infractions of this policy or those that appear accidental in nature are typically handled informally by electronic mail or in-person discussions. More serious infractions are handled via formal procedures. In some situations, it may be necessary to suspend account privileges to prevent ongoing misuse while the situation is under investigation. Infractions by students may result in the temporary or permanent restriction of access privileges, notification of a student's academic advisor and/or referral of the situation to the Office of the President.

Those by a faculty or staff member may result in referral to the department director or administrative director. Offenses which are in violation of local, state, or federal laws may result in the restriction of computing privileges, and may be reported to the appropriate law enforcement authorities.

Reassessment of Plan

This Plan is reviewed at least annually and adjusted as needed. The President shall circulate this policy to the school's advisory board and request a reassessment. The annual review includes identification and assessment of internal and external risks to the security, integrity, and confidentiality of non-public personally identifiable information, including review of outside contractors and their contracts to ensure that proper safeguards are in place.

Employee Guidelines for Securing Covered Data and Information

"Covered Data" is defined as educational records, and the personal and financial information of students, prospective students, faculty members, staff members, alumni, customers and patients. When in doubt as to whether a piece of data or information is to be safeguarded as covered data and information, school employees/contractors will err on the side that it is covered data and information. Covered data and information includes both paper and electronic records. Examples of personal and financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories, and social security numbers.

Every school employee who has access to covered data and information is responsible for:

Maintaining physical security by locking rooms and/or file cabinets where covered data and information is stored.

1. Maintaining adequate key control and limiting access to sensitive areas to those individuals with a "need to know" in order to perform their job.

2. Using and frequently changing passwords to access automated systems that process covered data and information. Also encouraging the use of “strong” passwords (e.g. at least 8 characters, and not easily guessable). Also encouraging the safeguarding of passwords (e.g. do not leave passwords written down in easy view of others in the vicinity of an employees work area).
3. Using firewalls and encrypting covered data and information when appropriate and feasible.
4. Referring calls and mail requesting covered data and information to those individuals who have been trained in safeguarding covered data and information for these types of requests.
5. Shredding and erasing information when no longer needed in accordance with school policy.
6. Taking reasonable efforts to limit the view of computer screens and other mediums (e.g. paper) displaying covered data and information to only those employees who have a “need to know” in order to perform their job.
7. Closing covered data and information from computer screens when it is no longer in use. And never leave your desk area with covered data and information still displayed on a computer screen or on some other medium (e.g. paper) on the desk in clear site of a casual passerby.
8. Encouraging employees to report suspicious activity to supervisors and/or the President, as appropriate.
9. Encouraging password-activated screen savers and using them when an employee is away from his/her desk.
10. Taking reasonable steps to ensure that all future contracts are with service providers that are capable of maintaining appropriate safeguards for the covered data and information at issue.

▪

Disciplinary measures (including job termination) may be taken against any employee who intentionally, or through gross negligence, violates any of the above guidelines.