Texarkana College Information Security Policy

Contents

I. Purpose

Information security policy provides guidance and defines responsibilities and procedures related to the operational implementation of the College's information security program. This policy provides requirements and guidelines to: establish accountability and acceptable practices regarding the use and safeguarding of the College information resources; protect the privacy of personally identifiable information contained in the data that constitutes part of its information resources; ensure compliance with applicable policies and state and federal laws regarding the management and security of information resources; and educate individual users with respect to the responsibilities associated with use of the College information resources.

This Policy serves as the foundation for the Texarkana College Information Security Program and provides the authority to implement a successful program.

II. Policy Statement

College information is a valuable asset and requires appropriate protection. Unauthorized use or disclosure of the College data protected by laws, regulations, or contractual obligations could cause severe harm to the College and could subject the College to fines.

To manage these risks, the College must ensure that their information assets which store, transmit, or process College information, or can impact the security of the data, meet the information security processes and standards contained in this policy, and all pertinent laws, regulations, or contractual obligations.

III. Policy Objectives

The purpose of this Information Security Policy is to protect College information assets from all threats, whether internal or external, deliberate, or accidental. The increasing need to transmit information across networks of computers renders data more vulnerable to accidental or deliberate unauthorized modification or disclosure. Texarkana College information security objectives are to ensure:

Confidentiality of Data or Systems
The confidentiality of data is to be maintained at all levels of data processing cycles, whether it is in use, in motion, or at rest. The information is protected against unauthorized access through means of technical and manual controls appropriate for the type of asset.

Integrity of Data or Systems
The integrity of information is maintained through tools, techniques, and processes which provide adequate assurance that systems are free from unauthorized manipulation. Unauthorized manipulation may compromise accuracy, completeness, and reliability of data or system.

Availability
Availability of systems addresses the processes, policies, and controls used to ensure authorized users have prompt access to information. This objective protects against intentional or accidental attempts to deny legitimate users' access to information or systems.

Accountability
Accountability ensures business, regulatory and legislative requirements for information security are met. Specific processes and procedures comprising accountability prescribe:

- Information security related breaches, actual or suspected, are reported and investigated according to criticality and possible impact.
- Adequate information security training is provided to staff according to the level of their responsibilities related to the protection of information assets. Staff is aware of their accountability and that failure to comply with the information security policy is a disciplinary offence.
- Requirements are defined to prepare standards, guidelines, and procedures to support information policy objectives; and
- External organizations the College shares information with adopt and adhere to principles and procedures that meet regulatory requirements.

IV. Applicability

This Policy applies to:

- Information resources owned, leased, operated, or under the custodial care of the College.
- Information resources owned, leased, operated, or under the custodial care of third parties operated on behalf of the College; and
- Individuals accessing, using, holding, or managing the College information resources on behalf of the College.

The scope of this policy generally covers all employees, staff, contractors, and service providers that may have access to electronic assets and associated controls.

V. Enforcement

Employees must report known non-compliance with any requirement of this policy to the College Information Security/ IT Department.

Individual College employees who do not comply with this policy or the College information security standards may be denied access to College IT resources and may be subject to disciplinary action up to and including termination.

VI. Compliance

The College must ensure compliance with applicable state and federal laws and policies regarding the management and security of information resources.

VII. Information Security Standards

1 Account Management

All accounts that access College information resources must follow an account creation process associated with their job function based on least privilege. This process shall document who is associated with the account, the purpose for which the account was created, and who approved the creation of the account. Accounts requiring access to college information resources must have the approval of the owner of those resources. Accounts are to be created and managed using the following required account management practices.

1.1 Employee Account

The HR department must inform the IT department and respective application / information owners when an employee is hired, terminated, resigns, retires, or transfers so appropriate actions may be taken to secure the account and protect information resources.

1.2 User Account Updates and Revocations

Changes in user job function or status must be communicated to the system owner and Information Technology in the following cases:

- An employee resigns, retires, is deceased, or transfers to another position.
- The account is no longer needed.
- Other factors that change information system usage or need-to-know.
- A student who works for the College has a change in status.

Proper procedure must be followed to remove, disable, or otherwise secure associated accounts from College information systems.

1.3 Access Rights Review

Accounts must be reviewed at least annually to ensure their current state is correct.

1.4 Access Enforcement

Access to information resources must be appropriately controlled and managed.

- Users must be authenticated by user IDs, in conjunction with a strong password, and an approved authentication mechanism before they can gain access to the target system.
- Users of information systems must have a unique ID that is authorized for accountability purposes.
- Role-based access control must be used where possible.

1.5 Administrative Accounts

The allocation and use of administrative accounts must be restricted and controlled. The following steps should be considered:

- Special privileges must be allocated to users on an as needed basis and should be approved by the information resource owner.
- Individuals who use administrator or special access accounts must use the account or access privilege most appropriate for the requirements of the work being performed (e.g., user account vs. administrator account).

- All access via administrative accounts must be logged into the system management service to ensure proper accountability and transparency.

1.6 Separation of duties

Separation of duties must be implemented such that operational information resource functions are separated into distinct jobs to prevent a single person from harming a development or operational information resource or the services it provides, whether by an accidental act, omission, or intentional act.

Some other measures should be taken for the Account Management process.

- Password aging and expiration dates must be enabled on all accounts created for outside vendors, external contractors, or those with contractually limited access to the College information resources.
- All non-student/non-faculty logon IDs that have not been active within a period of 90 days shall be disabled.
- Faculty accounts that are no longer actively teaching or preparing for a course shall be disabled within 30 days of last class day.
- Accounts for transferred employees must have access required for previous positions removed and new access assigned based on the new position. If an employee must continue to support a previous position, up to a 30-day extension during the transition period may be granted. For longer periods, exceptions may be allowed based on business need.
- When a student worker is no longer an employee, all access to the information resources must be removed.

2 User Responsibilities and Accountability

Information owners, custodians, and users of information resources must be identified, and their responsibilities defined and documented by the College. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles.

2.1 Information Owner Responsibilities

The owner, or his or her designated representative(s), is responsible for:

- Classifying information under their authority, with the concurrence of the College President or his or her designated representative(s), in accordance with College established information classification categories;
- Approving access to information resources and periodically review access lists based on documented risk management decisions;
- Assigning custody of information or an information resource;
- Coordinating data security control requirements with the ISO;
- Conveying data security control requirements to custodians;
- Providing authority to custodians to implement security controls and procedures; and
- Justifying, documenting, and being accountable for exceptions to security controls. The information owner must coordinate and obtain approval for exceptions to security controls with the Information Security Officer; and participate in risk assessments.

2.2 Information Custodian Responsibilities

Custodians of information resources, including third party entities providing outsourced information resources services to the College must:

- Implement controls required to protect information and information resources based on the classification and risks specified by the information owner or as specified by the policies, procedures, and standards defined by the College Information Security Program;
- Provide owners with information to evaluate the cost-effectiveness of controls and monitoring;
- Adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;
- Provide information necessary to provide appropriate information security training to employees; and
- Ensure information is recoverable in accordance with risk management decisions.

2.3 End User Responsibilities

The user of an information resource shall:

- Use the resource only for the purpose specified by the College or information owner;
- Comply with information security controls and College policies to prevent unauthorized or accidental disclosure, modification, or destruction of data; and
- Formally acknowledge that they will comply with the security policies and procedures in a method determined by the institution head or his or her designated representative.

College information resources designated for use by the public must be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice prior to use.

3 Information Resources Acceptable Use

The Acceptable Use Agreement must address the following User responsibilities and behaviors:

- Ownership of the College information resources and data, including data maintained or created on a User's personal devices;
- Incidental use of information resources, including impact of placement of personal data on the College information resources;
- User's expectations with regards to the privacy of information stored or created on the College information resources; and
- User's responsibilities with respect to maintaining the security, integrity, and, as applicable, confidentiality of the College information resources.

Texarkana College is responsible for ensuring that each user who is employed by the College or who provides services to or on behalf of the College acknowledges awareness of the existence of and the User's responsibility for complying with the College Acceptable Use Agreement.

4 Password Management

Strong passwords shall be used to control access to the College information resources. The allocation of passwords must be controlled through a formal management process. The College's Password Management Standard must be followed when assigning passwords to user accounts. Users should also be made aware of the significance of the password and their responsibility for taking appropriate measures to protect passwords from misuse.

All account passwords associated with the College information resources must be constructed, implemented, and maintained according to the following, as technology permits:

4.1 Initial Password

Employees are provided with an initial secure random password via a secure procedure during the Human Resources on-boarding process.

4.2 Standard Account

Standard account passwords must comply with the following password strength requirements:

- Minimum standard of 16 characters with complexity enabled.
- Include a varied set of characters to include three of the four: one special character, one number (0-9), one uppercase letter and/or one lowercase letter.
- Account users do NOT need to change their password unless there is suspicion that it has been compromised.
- Recovery
-

4.3 Password requirement (Service Accounts)

Where it is practical, Group Managed Service Accounts will be used in place of traditional service accounts.

- minimum standard of 16 characters with complexity enabled.
- service account passwords should be randomly generated.
- service accounts should be changed when a person exposed to the password leaves the organization.

4.4 Password requirement (Privilege Level/Administrative Accounts)

Administrator and privilege users' passwords must be constituted by keeping the following baseline:

- Minimum standard of 16 characters or maximum length allowed by the device with complexity enabled.
- must be hard to guess.
- privilege/admin users should change their password on or before password expiry policy setting of 91 days.
- MFA for administrative accounts.

4.5 Password Security

Passwords must be stored, transmitted, and displayed in a secure manner. Accounts that have been suspended or locked because of suspected misuse or compromise shall require password resets, with the assignment of a new unique password before reactivation.

4.6 Default/Blank Password

Default vendor passwords must be altered following installation of systems or software.

4.7 Unsuccessful Logon Attempts

An account lockout mechanism must be used for all the College accounts unless specifically not supported by the application. Standard accounts lock out after six unsuccessful attempts and accounts reset for two minutes.

4.8 Password History

The security setting in each production system must determine the number of unique new passwords that have to be associated with a user account before an old password can be reused. Recommended password history to be enabled is last 24 passwords.

4.9 Vetting User identity

Users must provide proof of identity at any time a password is issued or reset via a secure mechanism.

College identity credentials (security tokens, security certificates, smartcards, and other access and identification devices) must be disabled or returned to the appropriate department or entity on demand or upon termination of the relationship with the College.

5 Remote Access

The standard and controls govern remote access to users connecting to the College's network over public switched networks, the Internet, or other remote networks. These controls are designed to minimize the potential exposure to the College's information systems from damage which may result from unauthorized access to information resources, thus ensuring confidentiality and integrity.

- Information owners/supervisors are responsible for authorizing access to information resources and notifying the Information Technology Department when requirements change.
- All sensitive data transferred over a remote access link must be encrypted using strong encryption.
- Firewall policies must be configured to limit access to required services and systems.
- Audit logs must be enabled and stored on a central log server and reviewed for violations.
- Remote access to business information across public networks must be restricted to approved devices and only take place after successful identification and authentication.
- In cases where a vendor requires remote access to provide support services, procedures must be followed to ensure proper authorization, authentication, and encryption.
- Remote Access to vendors must be limited to the minimum level required for performance of the requested support and activity must be appropriately monitored wherever possible.
- All remote access to networks owned or managed by College System must be accomplished using a remote access method approved by the College or System, as applicable.
- Only College approved devices (laptops) are allowed to remote VPN into information systems and that remote access must be approved.

6 Wireless Access

The wireless local area network (WLAN) enables access to computing resources for devices not physically connected to a network. Wireless networks must meet the following requirements:

- Service Set Identifiers (SSID) values must be changed from the manufacturer default setting.
- Unauthorized access points and network attached wireless devices are prohibited on the College network.
- Wireless network configurations must be documented and be periodically compared and reviewed against the approved configuration documentation.
- Access to the wireless network must be authenticated by the College IT approved methods.
- Wireless users must comply with all applicable College requirements.

7 Publicly Accessible Content

The College must develop procedures to post information on publicly accessible information resources to ensure only authorized College personnel may post public content.

- Only authorized personnel specifically authorized to post information to publicly available College sites may publish public content.
- Authorized personnel must be trained to ensure that publicly accessible information does not contain non-public information and appropriate procedures followed to prevent accidental posting of non-public information.
- The content on the publicly accessible information system must be periodically scanned for non-public information and removed if any such information is discovered.

8 System Use Notification

All information systems must display an acceptable use notification message or banner before logging in to the information system. The login notification must address the following items:

- Unauthorized use is prohibited;
- Usage may be subject to security testing and monitoring;
- Misuse is subject to criminal prosecution; and
- Users have no expectation of privacy except as otherwise provided by applicable privacy laws.

9 Media Handling and Disposal

Proper media handling processes prevent unauthorized disclosure, modification, removal, or destruction of College information assets, and interruption of business activities. Media containing confidential or sensitive data must be controlled and physically protected. Appropriate procedures must be established to protect documents, computer media (e.g., tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

- Only College approved media must be used.
- Removable media containing confidential data must be encrypted.
- Media must be stored in a safe and secure environment.

- Media containing sensitive information such as backups or archived disks must be clearly labeled and tracked.
- Only authorized College staff may send media outside of the campus.

Disposal - Media must be disposed of securely and safely when no longer required, using formal procedures. The procedures for secure disposal of media containing sensitive information must be commensurate with the sensitivity of that information. The following items must be considered:

- Procedures must be in place to identify the items that might require secure disposal.
- Media containing sensitive information must be stored and disposed of securely and safely, e.g., by incineration or shredding.
- If no longer required, the contents of any reusable media that are to be removed from the College must be made unrecoverable.
- Any unused or expired storage media must be sanitized and sent to the third-party for shredding and certification of proper disposable obtained.
- Where necessary and practical, authorization must be required for media removed from the College and a record of such removals must be kept maintaining an audit trail.

10 System Development Life Cycle

Information security should be considered throughout the life of the information system, including development, programming, configuration, or operational changes and modifications.

The information resource owner is responsible for ensuring that all requirements of this Control are substantiated and maintained throughout the life cycle of an information system.

- All information systems must be designed, developed, configured, and operated within a security framework that ensures confidentiality, integrity, and availability throughout the information system life cycle.
- Information security roles and responsibilities are defined and documented throughout the system development life cycle.
- Applied security controls shall be based on the classification of data that is stored or processed by the software or information system.
- Risk management must be fully integrated into the life cycle from conception to development to operation and then finally to disposition.
- Assessment of information security risk, security testing, and audit controls shall be included in all phases of the system development life cycle or acquisition process to produce the desired outcome with respect to meeting the security requirements for the system.
- The information resource owner shall approve and document that the information system is operationally secure and acceptable for use.
- Security reviews shall be conducted when an information system has been modified or updated to ensure that the security posture of the information system has not been compromised.

11 System / Service Acquisition

Texarkana College must ensure that security is an integral part of all development and acquisitions throughout the lifecycle. Information systems include operating systems,

infrastructure, business applications, off-the-shelf products, services, and user-developed applications.

- The College must adopt standards and/or procedures to ensure that the protection of Information Resources (including data confidentiality, integrity, and availability) is considered during the development or purchase of new information systems or services.
- Authorization is received from appropriate management before new information systems (e.g., servers, network devices, etc.) are placed into the production environment.
- The Information Security Officer shall review security requirements, specifications, and, if applicable, third-party risk assessments for any new system, applications, or services that are mission critical or that receive, maintain, and/or share Confidential data.
- Security requirements must be identified, documented, and addressed in all phases of development or acquisition of information resources.
- The College determines, documents, and allocates as part of its capital planning process, resources required to adequately protect the information system.
- The College must include applicable security requirements either explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws and standards.
- Employees responsible for configuration and management of information systems must incorporate security considerations. Necessary training, vendor documentation, and configuration requirements must be incorporated as part of the process.
- Test environments where possible must be kept either physically or logically separate from production environments.
- Outsourcing contracts must be developed and reviewed with the third party and cloud computing service provider.

12 User Installed Software

- All software installed on College owned or operated computer systems used by faculty members, staff members, agents, or students in the conduct of College business must be appropriately licensed.
- All software installations must be performed by the IT Department. Software may not be copied or installed by other faculty, staff, or students. If software is needed that is not part of the default suite supplied by the College, the software will be installed by IT staff after appropriate approval has been granted.
- The IT department must maintain documentation (e.g., End User License Agreements, purchase receipts, etc.) to validate software is appropriately licensed.

13 Security Awareness and Training

Security awareness is an integral part of the College Security Strategy. End-users are made aware of security threats and how those threats may be used to compromise data under their control.

- All employees/contractors with access to the college information resources must participate in Cybersecurity awareness training.

- All new employees are required to sign a data security agreement and acknowledge they have read, understand, and will comply with requirements regarding computer security policies, standards, and procedures.
- In addition to initial training, owners and custodians must receive periodic training addressing the responsibilities associated with their roles. Method of delivery and scheduling of such training must be determined by the College.
- Security awareness training must address recognition and reporting of indicators for insider threats.
- IT personnel/ISO must establish and maintain security awareness techniques such as generating email advisories or publishing on websites.
- HR must maintain records of all the staff who have completed security training and maintain those records for compliance purposes.

14 Risk Management

Information security risk assessment is the process used to identify and understand risks to the confidentiality, integrity, and availability of information and information systems.

14.1 Risk Assessment of Internal Resources

Risk assessment consists of the identification and valuation of assets and an analysis of those assets in relation to potential threats and vulnerabilities, resulting in a ranking of risks to mitigate. The resulting information should be used to develop strategies to mitigate those risks.

- Accurate inventory of information resources and associated owners must be maintained.
- Risk assessments must be performed annually, and results must be documented.
- Information Resources Owners in consultation with information security personnel and the IT Custodian:
    - define, approve, and document acceptable risk levels and risk mitigation strategies; and,
    - conduct and document risk assessments to determine risk and the inherent impact that could result from their unauthorized access, use, disclosure, disruption, modification, or destruction.
- Risk acceptance decisions relating to acceptance of risk must be documented and are to be made by the Information Resource Owner, in consultation with information security personnel, for resources having a residual risk.
- Custodians of information resources must implement approved risk mitigation strategies and adhere to information security policies and procedures to manage risk levels for information resources under their care.
- The risk assessment must be updated whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
- The Information Security Office must implement a technical Vulnerability Management Program in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

14.2 Risk Assessment of Third-party Service Providers

- A risk assessment of a third-party service provider is required if the provider processes or stores confidential data (HECVAT, HECVATE LITE, etc.).

15 Third-Party or Cloud Computing Services

- A risk assessment for a third-party service provider or cloud computing services must be performed and proper system or service acquisition procedure must be followed.
- The Data Owner and staff with the ISO review contracts to determine whether the contract involves third-party access to, outsourcing, maintenance, or creation of College confidential data; and that all such access, outsourcing, or maintenance fully complies with applicable standards.
- The assessment must include copies of requested self-assessments or third-party assessments of the integrity and reliability of the vendor's security profile.
- Vendors must verify technological, administrative, and physical safeguards are in place to ensure the confidentiality, security, and integrity of the data at rest and during any transmission or transfer.
- Confidential information, including PII, may be managed by a cloud service/third party only when there is a contract in place with the College.
- Information Resource Owner ensure outsourcing contracts shall address the following requirements:
    - security, backup, confidentiality, and privacy requirements;
    - right for the College to conduct a security assessment or a right to audit security assessments performed by third parties;
    - third parties and cloud computing services must adhere to all Federal and State laws pertaining to the protection of information resources and privacy of confidential data.
    - third parties and cloud computing services shall agree and understand that data may be subject to e-discovery and Texas state auditing and requests for public information requirements;
    - acceptable methods exist for the return, destruction, or disposal of confidential information in the third party or cloud computing service provider possession at the termination of the contract; and
- In the event of any unauthorized use or disclosure of any confidential data occurs, the vendor must provide information to the College about the breach.
- Texas Government Code 2054.0593 mandates that state agencies as defined by Texas Government Code 2054.003(13) must only enter or renew contracts to receive cloud computing services that comply with TX-RAMP requirements beginning January 1, 2022.
- Only cloud computing services, as defined by the Texas Government Code, section 2054.0593(a), are within scope for TX-RAMP. Products or services that are not cloud computing services are not subject to TX-RAMP. Certain specific cloud computing services are outside of the scope of Texas Government Code, section 2054.0593 and, as such, are not required to comply with TX-RAMP.
- Cloud providers need to demonstrate compliance with the security criteria to receive and maintain a certification for a cloud computing service.

16 System and Information Integrity

The Information Security Officer in coordination with Information Resource owners/custodian, must develop and document a set of controls that addresses the System and Information Integrity of information resources. These controls should include purpose, scope, roles, responsibilities, management commitment, coordination among college entities, and compliance. The ISO shall review and update the System and Information Integrity controls as necessary.

16.1 Malicious Code Protection

Malware prevention employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

- Computer systems owned by the College must be kept current with security updates released by the manufacturer of the appropriate operating system, and/or application software (e.g., patched and updated).
- Software no longer supported by the manufacturer is not permitted except in the case of documented and approved business needs.
- Where feasible, personal firewall software or hardware must be installed to aid in the prevention of malicious code attacks or infections.
- E-mail attachments and shared files of unknown integrity must be scanned for malicious code before they are opened or accessed.
- Software to safeguard against malicious code (e.g., anti-virus, anti-spyware) must be installed, enabled, and functioning to protect information resources. Where possible and feasible, the automatic update feature of the software that safeguards against malicious code must be enabled.
- Software safeguarding information resources against malicious code must not be disabled or bypassed.

16.2 Security Monitoring

The purpose of the information system security monitoring is to ensure that information resource security controls are in place, effective, and not being bypassed. Security monitoring confirms that the security practices and controls in place are being adhered to and are effective. Monitoring consists of activities such as the review of user account logs, application logs, data backup and recovery logs, automated intrusion detection system logs, etc.

- Confidential information resource systems shall, at a minimum, enable operating system logging features.
- Co-relation of security events must be monitored through automated tools, e.g., a SIEM.
- Network traffic and use of information resources must be monitored only as authorized for the purpose of fulfilling the College mission.
- Intrusion Detection Systems (IDS) shall be used to monitor networks or systems for malicious activity or policy violations.
- Vulnerability assessments must be performed every quarter, at minimum, to identify software and configuration weaknesses within information systems.
- Training/awareness shall be provided for current threats.
- Data Loss Prevention (DLP) for email shall be used to prevent data leakage.
- Data Loss Prevention (DLP) for devices shall be used to discover and protect sensitive items.

17 Personnel Security

17.1 Position Risk Designation

The College identifies and classifies personnel positions based on risk category in order to determine the risk level associated with the position.

- The information system owner or manager, in conjunction with Human Resources, must assign a risk designation to all College positions within the unit (such as a security designation in a job description).
- The College Human Resources shall incorporate appropriate screening criteria for individuals hired for positions.
- All authorized users of the College information resource must formally acknowledge that they will comply with the security policies and procedures of the College.

17.2 Personnel Screening

The College screens individuals, to authenticate identity, before authorizing access to college information resources as specified in Texarkana College Board Policy Manual.

17.3 Personnel Termination

In the event of termination of individual employment, the College terminates information resource access and retrieves all College information system-related property. It is the responsibility of the Information Resource Owner / IT Personnel, in conjunction with Human Resources, to:

- disable information resource access within 72 hours after notification of termination;
- revoke the individual's College credentials;
- retrieve all College information resource property; and
- retain access to College information and information resources formerly controlled by the terminated individual for a period of no less than one year.

17.4 Personnel Transfer

The College reviews information resource/facility access authorizations when personnel are reassigned or transferred to other positions within the College and initiates appropriate actions as identified by Human Resources. It is the responsibility of the Information Resource Owner or manager, in conjunction with Human Resources, to:

- review and confirm ongoing operational need for current logical and physical access authorizations to information resources/facilities when individuals are reassigned or transferred to other positions within the College; and
- modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.

18 Security Incident Management

- Information Resources Owners, Custodians, and Supervisors or Managers who becomes aware of a security incident (e.g., unauthorized disclosure of personal information, malware, etc.) is to report the incident to the Director of IT and the Information Security Officer.
- Incidents must be handled as specified in the College's Incident Response Plan.

- The College must disclose, in accordance with applicable Federal or State law, incidents involving computer security that compromise the security, confidentiality, and/or integrity of Personal Identifying Information (PII).
- The Director of IT will notify senior management of any security events that must be reported to external entities.
- Security incidents that require timely reporting, the Director of IT along with the Information Security Officer must report the incident to the appropriate State and Federal agencies as required by governing laws, rules, and procedures.
- Monthly Incident reporting must be provided to the Department of Information Resources.
- Anyone observing known or suspected computer security violations must report the incident to the IT Service Desk for further investigation.

19 Physical and Environmental Security

All Information Resources must be physically protected based on risk.

19.1 Safeguards

The College must adopt safeguards to ensure appropriate granting, controlling, and monitoring of physical access. Physical access safeguards must incorporate procedures for:

- protecting facilities in proportion to the criticality or importance of their function and the confidentiality of any information resources affected;
- managing access cards, badges, and/or keys;
- securing and maintaining inventory of keys, combinations, and other physical access devices; and
- granting, changing, and/or removing physical access to facilities to reflect changes in an individual's role or employment status.

19.2 Data Center Security

The College must incorporate procedures for data center security, for both main site and remote disaster recovery site including:

- reviewing physical access periodically;
- designating staff who will have authorized access during an emergency;
- monitoring the exterior and interior of the facility 24/7;
- maintaining and monitoring appropriate environmental controls such as alarms that monitor heat and humidity, fire detection systems supported by an independent energy source, and uninterruptable power systems capable of supporting all computing devices in the event of a primary power system failure;
- Controlling visitor and vendor physical access to the data center with procedures that incorporate the following:
    - advanced scheduling, access logging, and documenting of visits;
    - escorting while on premises;
    - changing keys when lost and collecting them when individuals are transferred or terminated; and
    - restricting the unauthorized use of photographic and video devices while on premises.

19.3 Physical Security Incident Response

- In case of theft or vandalism the College has its own police that is available 24/7.
- Facility department must insure protection from water leakage or power outage.
- The college Infrastructure team is responsible for the maintenance of servers and devices.

20 Audit and Logging

The College must maintain and monitor system logs and retain logs in accordance with the College retention schedule where feasible (three months readily available for critical systems and one year searchable in SIEM when required).

20.1 Content of Audit Records

The information resource custodian must ensure logging mechanisms are in place to record user activities, exceptions, and information security events, including:

- date and time of the event;
- the software or hardware component of the information resource where the event occurred;
- source of the event (e.g., network address);
- type of event that occurred;
- user/subject identity (user, device); and
- the outcome (success or failure) of the event.

20.2 Audit Storage Capacity

The information resource custodian must allocate sufficient audit record storage capacity and configure auditing to reduce the likelihood of such capacity being exceeded.

20.3 Audit Processing Failure

The information resource custodian ensure that information resources are configured to provide alerts:

- in the event of an audit failure; and
- once the maximum storage capacity for audit logs is reached.

Audit Failure e-mail alert from information systems is sent to Information resource custodian and ISO.

20.4 Audit Review, Analysis, and Reporting

Information resource custodians and ISO are responsible for:

- reviewing and analyzing information resource audit records for indications of inappropriate or unusual activity; and
- reporting findings to information resource owner.

20.5 Time Stamp

The clocks of all relevant information processing systems within an organization or security domain must be synchronized with an agreed accurate time source.

20.6 Protection of Audit Information

Logging facilities and log information should be protected against tampering and unauthorized access and procedures should be in place to detect operational problems with the logging facility.

20.7 Audit Generation

The information resource custodian is responsible for configuring information systems to provide audit record generation capability for the list of auditable events on critical servers.

21 Data Classification

Owners of information resources must classify the data based on the College Data Classification Standard and must ensure the classification is properly maintained in the event the data classification changes. All designated custodians must ensure appropriate security controls are applied according to the classification of data.

Confidential Information

Description:

Information (or Data) is classified as Confidential if it must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreement.

Examples:

- Personally, Identifiable Information (PII) such as Social Security numbers (SSN) and/or financial account numbers.
- Student education records are protected by FERPA.
- Student Loan information subject to GLBA.
- Debit or credit card numbers.

Comments:

- This classification is reserved for information that is protected from public release based on state or federal law or binding legal agreement.
- This classification may not be absolute; context is an essential element.
- Owners of confidential information must ensure such information is correctly classified.
- Custodians of confidential information must implement appropriate controls.
- (In terms of the Federal Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, this category equates to HIGH IMPACT for a Confidentiality, Integrity, and Availability breach).
- Consult the Office of Institutional Advancement regarding confidential information requested through open records, subpoenas, or other legal processes.

Controlled Information

Description:

The Controlled classification applies to information/data that is not generally created for or made available for public consumption but may be subject to release to the public through request via the Texas Public Information Act or similar State or Federal law.

Examples:

- Non-public administrative or operational data (e.g., employee evaluations, asset listings and locations, etc.)

- Personnel Records.
- Internal meeting information.
- Non-confidential internal communications.

Comments:

- This classification encompasses that greatest volume of information within the College.
- (In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality, Integrity, and Availability breach).
- Consult the Office of Institutional Advancement regarding confidential information requested through open records, subpoenas, or other legal processes.

Public Information

Description:
Information/data that is freely and without reservation made available to public through posting to public websites, distribution through email, or social media, print publications or other media. This classification also includes information for which public disclosure is intended or required.

Examples:

- Unrestricted Directory Information.
- Educational content is available to the public at no cost.
- Public web posting.

Comments:

- Information can migrate from one classification to another based-on information lifecycle. For example, a DRAFT Tuition fee schedule would fit the criteria of "Controlled Information" until being published upon which it would become public information.
- (In terms of FIPS 199, this category equates to LOW IMPACT for a confidentiality breach.)

Systems storing College data will be assessed annually in a risk assessment where each system is classified based on the data it is associated with.

22 Backup and Disaster Recovery

The College data must be backed up in accordance with risk management decisions implemented by the data owner. Each backup plan must incorporate procedures for:

- recovering data and applications in case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or system operations errors;
- assigning operational responsibility for backing up of all servers;
- scheduling data backups and establishing requirements for off-site storage (cloud);
- securing on-site/off-site storage and media in transit, as necessary; and
- testing backup and recovery procedures.

22.1 Disaster Recovery Plan.

Owners of resources containing confidential data must adopt a disaster recovery plan commensurate with the risk and value of the information resource and a completed Business Impact Analysis. The disaster recovery plan must be periodically reviewed and updated whenever there is change in infrastructure and processes. The disaster recovery plan must incorporate procedures for:

- recovering data and applications in the case of events that deny access to Information Resources for an extended period (e.g., natural disasters, terrorism);
- assigning operational responsibility for recovery tasks and communicating step-by-step implementation instructions;
- testing the disaster recovery plan and procedures every year at minimum (example: tabletop or scenario testing, leveraging major scheduled upgrades, activating actual service outages in a controlled scenario; and
- making the disaster recovery plan available to all the stakeholders.

23 Configuration Management.

The information resource owner, or custodian shall develop, document, and maintain a current baseline configuration for information resources. The information resource owner, or designee, shall:

- establish mandatory configuration settings for components employed within the information resource and maintain the inventory;
- configure security settings of information resource components to the most restrictive mode consistent with operational requirements;
- change control procedure shall be followed for any changes and
- enforce the configuration settings in all components of the information resource.

23.1 Network Infrastructure

The network administrator shall be responsible for configuring and managing the network resources in accordance with the College security policies, standards and procedures by:

- segmenting the College network either physically or logically to reduce the scope of exposure of information resources commensurate with the risk and value of the information resource and data; and
- separating Internet-facing applications from internal applications;
- maintaining appropriate access to the network infrastructure in accordance with the College information security policies, standards, and procedures; and
- managing, testing, and installing updates to operating systems and applications for network equipment.

23.2 Server Hardening

To protect against malicious attack, all servers on College will be security hardened based on risk and must be administered according to policies, standards, and procedures prescribed by the College, as applicable, and must incorporate procedures for:

- setting baseline security “hardened” configuration standards for all servers; new servers must be hardened using industry recognized standards, e.g., vendor documentation, CIS, NIST, etc.;

- managing the testing and installation of service packs, hot fixes, and security patches;
- removing unnecessary services, software, and drivers;
- installing and enabling malware protection software on systems for which it is available;
- maintaining and tracking changes.

23.3 Device Configuration.

All devices (e.g., routers, laptops, tablets, desktops, and handheld devices) on College networks must be protected against malicious attack. The administrator shall:

- maintain baseline security hardened configuration standards for all devices;
- establishing and making available minimum-security configurations for college-owned and non-college owned portable computing devices; and
- recommended patch management practices.

23.4 Patch Management

- Prior to moving a new system into the production environment all patches must be applied.
- Operating system, application services, and network device security patches must be applied as soon as reasonably possible with consideration taken to the urgency of the patch. Patches will be applied in a manner consistent with the change management process.
- If a patch is available, the risks associated with installing the patch should be assessed (the risks posed by the vulnerability should be compared with the risk of installing the patch).
- When feasible, patches should be tested and evaluated before they are installed to ensure they are effective and do not result in side effects that cannot be tolerated; if no patch is available, other controls should be considered.
- The patch management process must include a rollback plan.

24 Change Management

Change management (CM) is the planning, coordinating, and controlling of the implementation of changes to the environment. Any change to the College IT infrastructure must have approval of the change management prior to its implementation. These changes include, but are not limited to hardware, software, configuration, or voice/data network.

- Whenever possible, the end user will be notified of changes following the steps contained in the change management procedures.
- Consistent with change management procedures, a change management log shall be maintained for all significant changes including emergency changes. All changes (where possible) must be tested before applying to the production environment. Change management log entries must contain at least the following information:
    - date of submission and date of change;
    - impact of change;
    - owner and custodian contact information; and
    - the nature of the change.

All custodians must implement and adhere to the College Change Management Procedure to ensure secure, reliable, and stable operations.

25 Portable Computing

- Mobile computing devices that access College information resources must be encrypted, patched/updated, and protected with anti-virus software and, if appropriate, a personal firewall.
- College Data created and/or stored on personal computers, other devices, and/or non-College databases should be transferred to College Information Resources as soon as feasible.
- College data created or stored on a user's personal computers, smart phones, or other devices, or in databases that are not part of College Information Resources are subject to Public Information Requests, subpoenas, court orders, litigation holds, discovery requests and other requirements applicable to College Information Resources.
- Unattended portable computers, smart phones, and other computing devices must be physically secured.

26 System and Communication Protection

The College must define and enforce requirements to protect data transmissions and system-to-system communications, including analyzing the identity of communicators.

- College shall establish a security strategy that includes perimeter protections (e.g., DMZ, firewall, intrusion detection or prevention system, or router) and incorporates:
    - monitoring for denial-of-service attack;
    - configuration settings at the network layer to combat such attacks; and
    - maintaining logs of network activity.
- Monitor and control the external boundary of the network and at key internal boundaries within the network.
- Implementing subnetworks for publicly accessible system components that are logically separated from internal college networks.
- Ensuring that connections to external networks or information systems occur only through managed interfaces consisting of boundary protection devices arranged in accordance with an approved security architecture.
- Internal system names and addresses on network should be hidden from external networks using NAT (network address translation).
- Ports and protocols that are permitted through firewalls, both inbound and outbound, are only provided for business purposes and shall be approved.
- Establish the approval process for updating or changing rule sets on firewall.
- Effective tools and processes must be in place to proactively detect and respond to security threats/events through (e.g., DLP, SIEM, NetFlow, etc.) and monitoring processes (e.g., alerts from IDS/IPS alert) for taking timely actions.
- Implementing DNS service in a manner that supports cryptographically signed responses and validates DNS results to reduce risk of traffic diversion through DNS spoofing; cache poisoning etc.
- DNS, IP, and port filters are used to reduce the risk of malware, block access to inappropriate content, and preserve bandwidth within the College network. First, all DNS requests are limited to only approved DNS servers that block known malicious domains. Second, all traffic is filtered by an IP address blacklist that is created from multiple reputable sources. Third, all traffic is limited to a set of specific ports required for common

Internet communication. Exceptions to the DNS, IP, and port filters require approval from IT Head.

- Encryption requirements for information storage devices and data transmissions, as well as specific requirements for portable devices, removable media, and encryption key standards and management, shall be based on risk management decisions.
  - Confidential information that is transmitted over a public network (e.g., the Internet) must be encrypted.
  - The minimum algorithm strength for protecting confidential information is an AES 128-bit encryption algorithm.
  - Manage cryptographic keys using automated mechanisms with supporting procedures where feasible.
  - Appropriately secure public/private keys and maintain availability of information in the event of the loss of cryptographic keys by users.
  - BitLocker keys are backed up securely on Active Directory.

27 Maintenance

The College Information Resources infrastructure is constantly changing and evolving to support the mission of the college computer networks, systems, and applications require planned outages for upgrades, maintenance, and fine-tuning.

All planned upgrades and maintenance take place after the change management process on Friday 12:00 am midnight to 7:00am using different system maintenance tools such as System Center Configuration Manager (SCCM), LibreNMS, etc.

All custodians must implement and adhere to the College Change Management process to ensure secure, reliable, and stable operations.

Vendor or other Third-Party Assessment. Prior to access, maintenance, or creation of the College Data by a Vendor or any other third-party, the Institution must perform an assessment to ensure that:

- the Vendor has sufficient technological, administrative, and physical safeguards to ensure the confidentiality, security, and Integrity of the data at rest and during any transmission or transfer; and
- any subcontractor or other third-party that will access, maintain, or create data pursuant to the contract will also ensure the confidentiality, security, and Integrity of such Data while it is at rest and during any transmission or transfer.

28 Privacy

The College must take all security measures, consistent with applicable laws, to protect personal information.

28.1 Personally Identifiable Information (PII)

- The College recognizes the special risks associated with the collection, use, and disclosure of social security, driver license, credit card and bank account numbers. PII must be stored as a confidential attribute associated with an individual, only if use of them is essential for the performance of a mission related duty.
- PII must be secured, and access restricted on a need-to-know basis.

- College must perform routine scanning and quarantining of PII to ensure it is protected from data leakage.
- Data Loss Prevention policies shall be enabled on email accounts to eliminate leakage of Personally Identifiable Information (PII).
- Data Loss Prevention policies shall be enabled on devices to discover and protect Personally Identifiable Information (PII).
- The College staff are advised not to use PII for testing and training purposes.
- Retention and Disposal of PII**-** PII shall be retained only for business need to authorized personnel and must be disposed securely after usage.

28.2 Information sharing with Cloud Service Provider/Third Party

- Confidential information, including PII, may be managed by a cloud service/third party only when there is a TX-RAMP agreement in place with the College.
- In the event of any unauthorized use or disclosure of any confidential data occurs, the vendor must provide information to the College about the breach.

28.3 Privacy Incident Response

- The College must notify privacy incidents in accordance with applicable Federal or State law, involving compromise the security, confidentiality, and/or integrity of Personal Identifying Information (PII).
- The Director of IT will notify senior management of any privacy security incident that must be reported to external entities.

28.4 Privacy Awareness and Training

- The College Cybersecurity training covers privacy module and all employees/contractors with access to the College information resources shall participate in cybersecurity awareness training.
- Email and advisories are sent to employees about protecting and not sharing PII.

The College detailed public privacy statement is available on the website regarding individual websites data collection, public forums, and links to other sites
https://www.texarkanacollege.edu/privacy/

29 Security Planning

The College must develop, disseminate, and periodically review/updates formal, documented procedures to facilitate the implementation of the Security Planning and associated Security Planning controls.

CIO/ISO shall report annually to the President on the adequacy and effectiveness of information security policies, procedures, and compliance with Texas Administrative Code, Chapter 202 and:

- Effectiveness of current information security program and status of key initiatives;
- Residual risks identified by the College risk management process; and
- College security requirements and requests.

The College ISO must develop and implement a security plan that provides an overview of the security requirements and a description of the security controls in place or planned for meeting those requirements.

ISO shall review the security plan for the information systems biennially and submit a report to DIR (Department of Information Resources) after senior management approval.

30 Security Assessment and Authorization

A review of the College information security program for compliance with Texas Administrative Code 202 standards will be performed at least biennially, based on business risk management decisions, by individuals independent of the information security program and designated by the College President or his or her designee. The security assessment will:

- review the College security controls and the environment of operation to determine the extent to which the controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the College security requirements;
- be performed by individuals independent of the Office of the Information Security; and
- be performed at least biennially.

The results of the security assessment shall be reported to the President or designated representative.

The College must authorize the information resource for processing before operations or when there is a significant change to the system.

31 Information Services Privacy

The purpose of this standard is to clearly communicate privacy expectations to the College information resource users. Internal users should have no expectation of personal privacy with respect to the College information resources.

Electronic files created, sent, received, or stored on computers owned, leased, administered, or otherwise under the custody and control of the College are the property of the College. These files may be accessed by authorized College IT employees and campus administration at any time without knowledge of the information resource user or owner.

They may also be accessed as needed for the purpose of system administration and maintenance; for resolution of technical problems; for compliance with the Texas Public Information Act; for compliance with Federal and State subpoenas, court orders, or other written authorizations; to conduct the business of the College; and to perform audits.

32 Security Control Exceptions

Exceptions to an otherwise required security control may be granted by the ISO/CIO to address specific circumstances or business needs, relating to an individual program or department, only as authorized by applicable law, and system and institutional policy.

Requests for exceptions of this type must be submitted and initiated by the Data Owner.

VIII. Definitions

Access- the physical or logical capability to view, interact with, or otherwise make use of information resources.

Availability- the security objective of ensuring timely and reliable access to and use of information.

Authentication - a process used to verify one's identity.

Backup - copy of files or applications made to avoid loss of data and facilitate recovery in the event of a system failure or other data loss event.

Cloud Computing- has the same meaning as "Advanced Internet-Based Computing Service" as defined in §2157.007(a), Texas Government Code

Control-A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Change Management - process of controlling the communication, approval, implementation, and documentation of modifications to hardware, software, and procedures to ensure that information resources are protected against improper modification before, during, and after system implementation.

Data - elemental units, regardless of form or media, that are combined to create information used to support teaching and other College business processes. Data may include but are not limited to physical media, digital, video, and audio records, photographs, negatives, etc.

Encryption-the conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Information-Data as processed, stored, or transmitted by a computer.

Information Resources - as defined in §2054.003(7), Texas Government Code "Information Resources" means the procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors.

Information System - an interconnected set of information resources under the same direct management control that shares common functionality. An information system normally includes, but is not limited to, hardware, software, network infrastructure, information, applications, communications, and people.

Information Security Program-the Policies, Standards, Procedures, Guidelines, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services adopted for the purpose of securing College information resources.

Information Technology (IT) - the hardware, software, services, supplies, personnel, facilities, maintenance, and training used for the processing of Data and telecommunications

Malware - a computer program that is inserted into an Information System, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of data, applications, or operating system, or of otherwise annoying or disrupting the User or Information System. Malware (malicious software) may attach itself to a file or application; deliver a payload without the

knowledge or permission of the User; insert itself as a service or process to intercept sensitive information and/or keystrokes and deliver it to a third-party; or compromise the user's computer and use it to launch compromises against other computers, among other capabilities. viruses, worms, Trojan horses, spyware, adware, ransomware, and any code-based entity that infects a host are examples of malicious software.

Password- a string of characters used to verify or "authenticate" a person's identity.

Passphrases and personal identification numbers (PIN) - serve the same purpose as a password.

Personally Identifiable Information (PII) - information that alone or in conjunction with other information identifies an individual. PII includes but is not limited to an individual's name; a Social Security number; a date of birth; a government-issued identification number; a mother's maiden name; unique biometric data (including an individual's fingerprint, voice print, and retina or iris image); a unique electronic identification number, address, or routing code; or a telecommunication access device.

Risk - the effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact. Risk outcomes are a consequence of Impact levels defined in this section.

Risk Assessment - the process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.

Risk Management - the process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures.

Remote Access - access to College information resources that originates from a remote location.

Security Incident - an event that results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate.

Standards-Specific mandatory controls that help enforce and support the information security policy.

Patch management - patch management is the process that helps acquire, test and install multiple patches (code changes) on existing applications and software tools on a computer, enabling systems to stay updated on existing patches and determining which patches are the appropriate ones.

Residual Risk - the risk (Low, Moderate, or High) that remains after security controls have been applied.

Server- a program that provides services to (programs on) other devices. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs**.**

Vendor - any third-party that contracts with Texarkana College to provide goods and/or services to the College.

SIEM- Security information and event management (**SIEM**) is an approach to security management that combines SIM (security information management) and SEM (security event management) functions into one security management system.

ISO- Information Security Officer ISO is responsible for overseeing the institution's information and data security.

Data loss prevention (DLP) - a set of tools and processes used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

DNS- DNS stands for Domain Name System. The main function of DNS is to translate domain names into IP Addresses, which computers can understand.

IX. Supplemental Forms, Plans and Procedures

All Security Forms, Plans and Procedures are available on request from IT.

- Security Review Access Form
- Employee Add/Modify Form
- Mobile Asset Form
- Security Access Request Form
- Disaster Recovery and Data Classification Approval Request Form
- Security Exception Request Form
- Change Management Form
- Incident Response Plan
- Disaster Recovery Plan
- Data Security Agreement

X. Contact Information

Questions or comments about this policy should be directed to Office of Information Technology

tcit@texarkanacollege.edu

XI. Revision History

Version	Date	Add/Remove	Comments
V 1.0			
V 2.0	10-23-23		
V 3.0	10/22/25	Added AI Policy	

AI Policy

I. Purpose & Scope Texarkana College is committed to responsibly integrating Generative Artificial Intelligence (GAI) to enhance education, administrative functions, and institutional operations while ensuring compliance with ethical standards, data security, and privacy regulations. This policy provides guidance on the acceptable use, governance, and oversight of AI within Texarkana College.

This policy applies to all faculty, staff, and students using AI tools in academic, administrative, or operational capacities. AI tools covered include institution-approved AI platforms, publicly available AI tools, and AI-enhanced software used in College-related activities.

Texarkana College recognizes that responsible AI integration must also comply with the Texas Responsible Artificial Intelligence Governance Act (HB 149, SB 1964, HB 3512) and accreditation standards outlined by SACSCOC. The policy therefore establishes institutional governance, risk management, and transparency protocols consistent with state and federal expectations.

What is Generative AI?

Generative AI (GAI) is a type of artificial intelligence that can create new content, such as text, images, music, or even code, by learning patterns from vast datasets. Unlike traditional AI, which is designed to recognize patterns and make decisions based on predefined rules, generative AI can produce original outputs by mimicking the structures it has learned.

These AI models are trained on large collections of data and use algorithms to generate content that closely resembles human-created work. Generative AI tools, such as ChatGPT and image generation software, are increasingly being used in education, business, and creative fields to assist with problem-solving, idea generation, and automation. However, the responsible use of these tools requires careful consideration of accuracy, ethics, and security.

II. Alignment with Institutional Goals This policy directly supports Texarkana College's 2024-2026 Strategic Plan by addressing the top priority of:

- **Success** – Establishing a team to assess best practices for the use of Artificial Intelligence (AI) and recommending policies and strategies for effective implementation into the curriculum.

By clearly defining guidelines, responsibilities, and acceptable uses, this policy ensures the strategic and thoughtful integration of AI tools to enhance student success and

faculty effectiveness, aligning closely with the college's commitment advancing our community through attainable higher education and lifelong learning.

The policy actively promotes responsible AI use through resources including the AI website, weekly faculty/staff workshops, and the Learning Technology Team on Microsoft Teams.

The College's AI Governance structure ensures that AI supports institutional effectiveness through annual AI Use Reports, training completion tracking, accessibility audits, and course-level policy alignment.

III. Guiding Principles Texarkana College encourages the adoption of AI while ensuring:

1. **Human Oversight** – AI should complement, not replace, human decision-making. Important decisions, particularly those affecting student outcomes or institutional policies, must remain subject to human oversight and verification.
2. **Privacy & Security** – AI use must comply with Texarkana College's Information Security Plan, the Family Educational Rights and Privacy Act (FERPA), and applicable Human Resources policies to ensure data protection, confidentiality and compliance with federal regulations and internal standards. Special care must be taken to protect sensitive information, maintain privacy, and secure institutional data when integrating AI tools.
3. **Transparency & Accountability** – Faculty, staff, and students must disclose AI use transparently where applicable, ensuring clarity on how and when AI tools are used in coursework, assessments, administrative functions, and communication. Proper documentation and attribution of AI-generated content are mandatory to maintain academic and operational integrity.

Transparency, Accountability, Accessibility, Security, and Human Oversight remain the core guiding principles in all AI applications. The College ensures that all AI use is tracked through approved systems, reviewed annually, and aligned with state mandates and accreditation standards.

IV. Acceptable Uses of AI

1. **Teaching & Learning**
    - Faculty may integrate AI into coursework to enhance learning, provided students are made aware of acceptable and unacceptable uses through course syllabi and classroom discussions.
    - AI tools may support personalized learning experiences, facilitate deeper understanding, and enhance creativity and innovation in teaching practices.

- Students must adhere to academic integrity standards when using AI in assignments, projects, and assessments.
- AI-generated work must be properly cited in accordance with institutional guidelines to ensure transparency and integrity.

Each course syllabus must include an "AI Use Statement" categorizing whether AI use is Allowed, Allowed with Citation, or Not Allowed. The Vice President of Instruction (CAO) oversees implementation and ensures consistency across divisions. AI tools used in instruction must meet accessibility standards; when not, Disability Services will ensure equivalent accommodations.

2. **Administrative & Operational Use**
   - AI may be used for workflow automation, student support services, and communication purposes.
   - AI may assist in data analysis and reporting, provided that usage strictly adheres to confidentiality and security protocols.
   - AI tools should **not** be used to process personally identifiable information (PII) without prior approval from the appropriate authorities, consistent with the Texarkana College Information Security Policy.

The Executive Director of IT (serving as CIO) must review and approve all new AI systems or vendor integrations to ensure compliance with FERPA, cybersecurity, and privacy laws. Vendor contracts must specify that institutional data cannot be used for model training without written consent.

Public Disclosure of AI Use

To ensure transparency, accountability, and public trust in the use of Artificial Intelligence, Texarkana College will disclose AI use wherever members of the public, students, or employees interact with AI-powered systems or communications.

1. Disclosure Requirements

- **All AI systems that engage with the public must clearly disclose their nature and purpose** at or before the point of interaction.
- A disclosure must include:
  - Identification that the user is interacting with an AI system;
  - The general purpose of the AI system (e.g., "to provide automated responses");
  - A caution that AI-generated responses may be incomplete or inaccurate;
  - A notice not to submit sensitive personal information (e.g., SSN, student ID, financial or medical details); and
  - A method for contacting a **human representative** for clarification or assistance.

Example Standard Banner:

“You are interacting with an AI-powered assistant. It generates automated responses based on approved data sources. Do not include sensitive or personal information in your message. A Texarkana College staff member can assist if needed.”

Example Footer Notice:

“This tool uses generative AI to assist users. Responses may not reflect official College policy. For verified information, please contact the appropriate department or visit texarkanacollege.edu."

2. Placement

- The short disclosure must appear at the entry point of all AI interfaces (e.g., chatbot welcome screen, helpdesk portal, or email autoresponder).
- The detailed disclosure must appear in the footer, transcript summary, or on a linked “AI Transparency and Privacy Notice” webpage.

3. Accessibility and Equity

- All disclosures must be **accessible** (WCAG 2.1 AA compliant) and readable at a 9th–10th grade level.
- Alternate formats (text-to-speech, captioning, or print statements) must be provided where required under ADA or Section 504.

4. Oversight

- The **Executive Director of IT (CIO)** oversees implementation and technical accuracy of disclosures.
- The **Vice President of Instruction (CAO)** ensures disclosures for instructional or learning systems meet academic standards.
- All disclosures must be **reviewed annually** by the **AI Governance Committee** and updated as technology or regulations evolve.

5. Legal Reference

- This disclosure section fulfills Texas HB 149 (2025), Section 5(b), requiring public entities to notify users when interacting with AI systems.

V. Prohibited Uses

- Using AI tools to fabricate, falsify, or misrepresent information (see Academic Dishonesty Policy).
- Inputting confidential student, faculty, or institutional data into unauthorized AI systems (see Information Security Policy).

- Relying solely on AI for high-stakes decision-making without human verification.
- Using AI-generated content without proper attribution.

In accordance with HB 149 (2025), Texarkana College also prohibits the development or deployment of AI systems that:

- Promote self-harm, violence, or criminal activity;
- Conduct "social scoring" or algorithmic classification that leads to unfair treatment;
- Perform biometric identification or data scraping without consent;
- Discriminate against protected classes or suppress lawful expression; or
- Generate or alter explicit or deepfake content involving or impersonating minors.

VI. Implementation & Compliance

- **Faculty Responsibilities** – Clearly define AI use policies in course syllabi, ensure students understand ethical considerations, and follow guidelines outlined in the Faculty Handbook.
- **Staff Responsibilities** – Ensure AI aligns with institutional policies, does not compromise data security, and adheres to guidelines outlined in the Catalog & Student Handbook 2024-2025.
- **Student Responsibilities** – Follow academic integrity guidelines outlined in this policy and in the Texarkana College Catalog & Student Handbook 2024-2025. Seek clarification before using AI tools.
- **Monitoring & Review** – The IT Technology Committee will oversee AI adoption, provide training, and update policies as necessary.

Tier	Definition / Description	Typical Examples	Governance Requirements
Tier 1 – Informational (Low Risk)	Systems that assist users with general information, tutoring, drafting, or analysis but do not access or store sensitive data and do not make autonomous decisions affecting individuals.	Chatbots answering FAQs, grammar checkers, image generators for instruction, summarization tools using public data.	• Department-level approval. • Disclosure of AI use to users. • Annual self-review by the area owner.
Tier 2 – Assistive (Moderate Risk)	Systems that support human decision-making or use limited	LMS-embedded AI grading suggestions, analytics	• Pre-approval by AI Governance Committee. • Data security review by IT.•

	institutional data (directory info, student ID numbers, or internal text) under human oversight.	dashboards, administrative automation tools.	Staff/faculty training required. • Annual review and accuracy/bias testing when applicable.
Tier 3 – Heightened Scrutiny (High Risk)	Systems that autonomously make or strongly influence consequential decisions involving eligibility, academic standing, or access to resources, or that process sensitive or protected data (FERPA, ADA, PII).	Predictive analytics influencing financial aid or admissions, AI-based proctoring, early-alert or retention algorithms, automated evaluation of performance.	• Mandatory Risk & Impact Assessment (RIA). • Bias testing and accessibility validation prior to deployment. • Human-in-the-loop review for all decisions. • Appeals process for affected individuals. • Annual audit by the AI Governance Committee. • Vendor contract must include "no model training on College data" clause.

Texarkana College hereby establishes an AI Governance Committee composed of:

- **Executive Director of IT (CIO)** – oversees security, data governance, and vendor oversight.
- **Vice President of Instruction (CAO)** – manages academic policy, syllabus integration, and instructional integrity.
- **Vice President of Administrative Services** – coordinates compliance and HR training accountability.
- **Legal Counsel (external or retained)** – provides legal review for contracts, FERPA, privacy, and statutory compliance.
- **Institutional Research/IE Representative** – ensures AI metrics are integrated into the College's Institutional Effectiveness cycle.
- **Registrar/FERPA Officer** – ensures privacy compliance.
- **Disability Services Representative** – ensures accessibility in AI-supported instruction.
- **HR Coordinator or HR Generalist** – monitors and reports AI training completion compliance.
- **Faculty and Student Representatives** – provide feedback and serve as liaisons for academic and student perspectives.

The AI Governance Committee meets quarterly to:

- Maintain an AI System Inventory;
- Classify systems by risk tier (Tier 1 Informational, Tier 2 Assistive, Tier 3 Heightened Scrutiny);
- Conduct annual risk and bias assessments;
- Publish an annual AI Use Report aligned with the Institutional Effectiveness cycle; and
- Review and update the AI Policy annually.

All employees and faculty must complete annual AI literacy training equivalent in scope to cybersecurity training. HR will track completion through the LMS and maintain records for audit.

Texarkana College will maintain a "Report an AI Concern" portal for employees, students, and the public. Alleged violations will be reviewed by the AI Governance Committee and, if necessary, referred to external legal counsel or the Texas Attorney General's Office per HB 149 enforcement procedures, which allow a 60-day cure period before penalties.

Annual reviews will ensure continued alignment with HB 149, SB 1964, HB 3512, and SACSCOC's *Good Practices in the Use of Generative AI*.

VII. Selected Available Resources

- A People's Guide to AI – A comprehensive guide to understanding AI, machine learning, and their societal implications.
- A Generative AI Primer – An introduction to generative AI and its impact on education.
- The Faculty Guide to Getting Started with Gen AI – 20 activities and 9 lesson plans developed in collaboration with UT Austin and Grammarly.
- Prompt Engineering Workshop – A searchable collection of prompts presented by the Texas Pioneer Foundation.
- Bringing AI to Schools – Guidance for school leaders on integrating AI into education.
- AI Bytes – AI4ALL Open Learning offers free AI curriculum and teacher resources.
- Critical AI Literacy – A curated collection of resources covering AI ethics, policy, and education.
- Harvard AI Code of Conduct – Harvard's student-developed AI Code of Conduct emphasizing responsible AI use.
- Syllabi Policies for AI – A collaborative resource for educators sharing AI syllabus policies.

- Artificial Intelligence and the Future of Teaching and Learning – A U.S. Department of Education report on AI in education.
- Daily Curriculum – A curriculum from MIT designed to educate students on AI fundamentals and ethics.
- Learn with AI – A toolkit for educators integrating AI into their teaching.
- Citing AI (APA) – APA guidelines for citing ChatGPT and other AI-generated content.
- TRAILS – A $20M NSF-funded initiative for ethical AI in law and society.
- AI Education Project – Resources for integrating AI into teaching at various levels.
- CRAFT – Free AI literacy resources for high school teachers.
- 101 Creative Ideas – A crowdsourced collection of AI applications in education.
- AI: A Guide to Thinking Human – A blog covering AI developments by Melanie Mitchell.
- Citing AI (MLA) – MLA guidelines for citing generative AI tools.
- Generative AI and the Transformer – An exploration of generative AI's impact on industries.