Texarkana College
Information Security Program

Overview

The Texarkana College Information Security Program (TCISP) intends to be a comprehensive information security program containing administrative, technical, and physical safeguards for the protection of customer information.

TCISP aims to meet the following objectives:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

Scope

TCISP applies to all Texarkana College employees, students, and contractors with access to records, documents, and information which contain sensitive or confidential information.

Definitions

Breach of system security means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner. *Texas Business and Commerce Code 521.053(a)*

Customer information means any record containing non-public personal information, as defined below, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the college district or its affiliates. *16 C.F.R. 314.2(b)*

Non-public personal information means:

1. Personally identifiable financial information; and
2. Any list, description, or other grouping of customers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. 16 C.F.R. 313.3(n)

Sensitive personal information means:

1. An individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted:
    a. Social security number;
    b. Driver's license number or government-issued identification number; or

c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

2. Information that identifies an individual and relates to:
    a. The physical or mental health or condition of the individual;
    b. The provision of health care to the individual; or
    c. Payment for the provision of health care to the individual.

"Sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government.
Business and Commerce Code 521.002(a)(2), (b)

Service provider means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provisions of services directly to the college district. *16 C.F.R. 314.2(d)*

Designated Program Coordinators

Chief Information Officer
Senior Programmer Analyst
Network Systems Administrator

Identification and Assessment of Risks to College Information

Texarkana College recognizes that it has both internal and external risks to the institution's information. These risks include, but are not limited to:

- Unauthorized access of confidential information by someone other than the owner of the covered data;
- 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; and
- Unauthorized transfer of covered data and information through third parties.

Texarkana College uses risk and privacy assessments to determine the likelihood and magnitude of harm that could come upon the institution in the event of a security breach. The college acknowledges that there are always risks, but seeks to place reasonable security safeguards in place to protect sensitive personal information. The college will use industry standard assessments like the SANS Top 20 and the Texas Cyber Security Framework to determine risk and strategies for securing data.

Employee Training and Management

Prior to being given access to sensitive personal information, new employees are required to review and sign the Texarkana College Information Technology Agreement (Appendix A). This agreement covers the importance and laws governing information security. All employees are required to participate in annual training that covers protecting sensitive personal information to comply with applicable laws and regulations.

Information Systems

Information systems, including network and software design, as well as information processing, storage, transmission and disposal are covered in the Access, Security and Control of Data and Information document (Appendix C) and other documents in the Existing College Information Technology Practices and Procedures section (page 5).

Incident Management

Appropriate College procedures shall be followed in reporting any breach of security or compromise of safeguards.

Information Safeguards

Administrative Safeguards

- Human Resources will conduct annual training on protecting sensitive personal information to comply with applicable laws and regulations
- Staff have been trained on the responsibilities in selecting passwords of appropriate strength, changing the passwords periodically (if required) and safeguarding their passwords
- When needed, staff are informed of current spam and phishing attempts

Technical Safeguards

- Secure protocols are used for sensitive personal data transmissions
- Technology resources (e.g., computers, laptops, applications and systems) that produce, maintain, transmit or permit access to College data or data entrusted to the College must be protected, at minimum, by an electronic account or other approved authentication mechanisms
- Each individual granted access to TC resources will be assigned his or her own unique electronic account(s) or authentication mechanism(s) for the purpose of accessing and using authorized information and/or resources. Except for the departmental accounts, discussed below, sharing of accounts is prohibited.
- Departmental accounts are accounts shared by multiple, but individually authorized individuals for a specific purpose, such as managing a departmental electronic mail account, system files and structures, or a computer that must operate in a continuous processing state. An account manager must be identified for each departmental or system account. The account manager must establish formal mechanisms for granting, tracking and terminating individual access and activity.
- Guest accounts may be provided to allow temporary access to College resources for a specific purpose and period. The parties authorizing and issuing the guest accounts must establish formal authentication, accountability and tracking procedures. All guest accounts must be created with an expiration date and time. Guest accounts must be disabled immediately upon the expiration date.

- An initial or reset password will be established or re-established using a unique, randomly generated password.
- An expiration date, of 90 days or less from the account activation date, must be established when setting up an account. Expired accounts must be locked, disabled or otherwise protected from unauthorized access.
- Systems must require users to change their passwords once every 90 days
- Systems shall include controls that prevent reuse of passwords during a 365-day cycle
- Passwords shall be at least eight (8) characters in length and 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.
- Systems that maintain or allow access to resources that house confidential, or business-limited information shall implement account lockout mechanisms, with the maximum failure limit set to five (5) attempts in order to minimize the risk that an unauthorized party will gain access to a resource using brute force or random, persistent guessing.
- 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.
- Passwords shall be masked during capture or keyboard entry
- All stored passwords will be encrypted.
- Authentication mechanism consisting of a user name and password shall require a password that is different from the user name. Blank usernames or passwords shall not be permitted.
- Files transmitted or carried off campus are encrypted
- Email is retained for a minimum of one year
- All internet traffic is processed by an intrusion detection system
- All servers and critical devices are scanned monthly for vulnerability assessments

Physical Safeguards

- Access to the data center is monitored by cameras at all times
- The data center is secured with a key fob providing access control and logging
- The data center is protected by universal power supplies and backup generator
- All network wiring closets are behind locked doors
- All network wiring closets contain a universal power supply
- All electronic media needing disposal are degaussed

Third-Party Vendor Agreements Concerning Protection of Personal Information

Texarkana College requires third-party vendors to follow at minimum the college's existing safeguards when having access to the sensitive personal information.

Information Security Program Review

TCISP will be periodically reviewed and adjusted in light of the results of testing and monitoring, any material changes to the college's operations or business arrangements, or any other circumstances that the college knows or has reason to know may have a material impact on the information security program.

Existing College Information Technology Practices and Procedures

Information Technology Agreement – Appendix A

This document consolidates several agreements into a single master agreement containing the Texarkana College Acceptable Use Agreement, the Texarkana College Information Security Agreement, the Texarkana College Confidential Information Agreement, and Texarkana College Media Release Agreement.

By signing this document, you are agreeing to abide by all applicable state and federal laws and college guidelines governing proper stewardship of data, software, and computing equipment you will have access to as an employee of Texarkana College.

FERPA

The Family Education Rights and Privacy Act of 1974, commonly known as FERPA, is a federal law that protects the privacy of student education records. Students have specific, protected rights regarding the release of such records and FERPA requires that institutions adhere strictly to these guidelines. Texarkana College annually informs students through an e-mail notification and our website about their rights as a student.

Acceptable Use – Appendix B

Under the provisions of the Information Resources Management Act, Texas Gov. Code Chapter 2054, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, the purpose of this document is to achieve the following:

A. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
B. To establish prudent and acceptable practices regarding the use of information resources; and
C. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Access, Security and Control of Data and Information – Appendix C

The purpose of this document is to establish procedures for the protection of the College computerized information systems, data, and software and to establish rights and responsibilities for the protection of staff and faculty who use these information systems.

Data Center Access – Appendix D

To ensure security measures are in place to protect Information Technology's data centers.

Data Protection – Authorization Controls Standard – Appendix E

The purpose of the Authorization Controls Standard is to provide guidance to those who are responsible for granting access to Texarkana College (TC) technology resources and data. The technology resources and data referred to in this standard include those owned by or entrusted to the College for the purpose of supporting academic, administrative, research or service related activities.

Electronic Account Standards – Appendix F

The purpose of the Electronic Account Standard is to provide a set of minimum operational and security related standards for electronic accounts that are used to identify individuals and authenticate access to Texarkana College (TC) data and technology resources. Generally, the electronic accounts used at TC consist of a username and password.

Electronic accounts are issued to students, faculty and employees for the purpose of conducting academic, research, service and/or administrative activities that support the College's mission. Periodically, other parties such as contractors, vendors, library patrons and guests are issued an electronic account for a limited period or purpose to support a College resource, use a service provided by the College or to participate in a College sponsored activity.

Appendix A

TEXARKANA COLLEGE

Department of Human Resources

Texarkana College Information Technology Agreement

This document consolidates several agreements into a single master agreement containing the Texarkana College Acceptable Use Agreement, the Texarkana College Information Security Agreement, the Texarkana College Confidential Information Agreement, and Texarkana College Media Release Agreement.

By signing this document, you are agreeing to abide by all applicable state and federal laws and college guidelines governing proper stewardship of data, software, and computing equipment you will have access to as an employee of Texarkana College.

Major Points of the Agreement

- You will protect and handle with diligence confidential Personally Identifiable Information (PII) belonging to students and employees.
- You will adhere to U.S. copyright law especially as it relates to software piracy.
- You will not deliberately or maliciously delete, alter, compromise or otherwise harm data required for the college's business or required for public record. This includes data contained in the college's databases, instructional material and records, business information, and business critical emails or emails required for public record.
- You will not disclose information not required by law that will adversely impact the college's revenues or goal of maximizing enrollment and student success. Requests for data by outside entities must be approved and conform to proper legal requirements prior to being granted.
- You will keep personal login credentials and data access control secure and secure equipment when not in use by logging off or locking the system to prevent unauthorized access. You are in violation if you share your credentials or use someone else's credentials to access resources.
- You will only access data as required to fulfill your assigned role. Looking up information on students or employees for reasons not related to your job is prohibited.
- You will protect access to computing equipment, mobile devices, and storage media belonging to the college or containing data obtained through employment with the college. All resources assigned to you must be returned upon termination of your employment with the college.
- You will not use computer resources for activity that would reflect negatively on the college's image.
- You will adhere to all policies and procedures placed in force by the Texarkana College Board and/or the President of Texarkana College.

State and federal laws covered by this agreement:

The following laws are referenced in various subtitles of this document. Many of these laws prescribe harsh penalties for violation and in some instances the penalties proscribed by law are listed. **References to fines, imprisonment, etc. that you find in this document are listed so that you are aware of the severity of the penalties**. You agree to adhere to all federal and state laws currently in force or subsequently enacted.

- Texas Government Code Chapter 2054, Information Resources Management Act
- Texas Administrative Code 202, Information Resource Standards
- Texas Penal Code, Chapter 33, Section 1, Title 7
- Texas Government Code, Chapter 552, Subchapter 1
- Family Education Rights and Privacy Act of 1974 (FERPA)

- Gramm-Leach-Bliley Act (GLBA)
- Federal Export Technology Control Laws
- Health Insurance Portability and Accountability Act of 1996 (HIPPA)
- Payment Card Industry Data Security Standard (PCIDSS)
- Sarbanes Oxley Act (SOX)
- U. S. Copyright law

Additional References

The Texarkana College Information Security Program (TCISP) is maintained on the Information Technology page of the Texarkana College website. Due to the evolving nature of Information Technology, you are to monitor and adhere to information posted on the website.

Texarkana College Acceptable Use Agreement

1. Introduction

Under the provisions of the Information Resources Management Act, Texas Gov. Code Chapter 2054, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this agreement is established to achieve the following:

A. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
B. To establish prudent and acceptable practices regarding the use of information resources; and
C. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

2. Application of Agreement

The Acceptable Use Agreement applies equally to all individuals granted access privileges to any College Information Resources, including students and guests.

3. Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the College are the property of the College and the State of Texas.

4. Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of College are not private and may be accessed by Information Technology employees at any time without the knowledge of or notice of Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

5. Protocol

A. Users must report any weaknesses in College computer security, any incidents of possible misuse, or any violation of this agreement to the CIO and other College officials as appropriate.
B. Users must not attempt to access any data or programs contained on College systems for which they do not have authorization or explicit consent.
C. Users must not share their College account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.

D. Users must not make unauthorized copies of copyrighted software.

E. Users must not use non-standard shareware or freeware software without IT approval unless it is on the College standard software list.

F. Users must not:

1. Purposely engage in activity that may harass, threaten or abuse others;
2. Deprive an authorized College user access to a College resource;
3. Obtain extra resources beyond those allocated, or;
4. Circumvent College computer security measures.

G. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, College users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on College Information Resources.

H. College Information Resources must not be used for personal benefit.

I. Users must not intentionally access, create, store or transmit material that the College may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the College's official processes for dealing with academic ethical issues).

J. Access to the Internet from a College-owned, home-based, computer must adhere to all the same policies that apply to use from within College facilities. Employees must not allow family members or other non-employees to access College computer systems.

K. Access to the College network from a personally-owned, home-based, computer or other device must adhere to all the same policies that apply to use from within College facilities. Employees must not allow family members or other non-employees to access College computer systems.

L. Users must not otherwise engage in acts against the aims and purposes of the College as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

6. Incidental Use

As a convenience to the College user community, incidental use of Information Resources is permitted with the following restrictions:

A. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, etc., is restricted to College approved users; it does not extend to family members or acquaintances.

B. Incidental use must not result in direct costs to Texarkana College.

C. Incidental use must not interfere with the normal performance of an employee's work duties.

D. No files or documents may be sent or received that may cause legal action against, or embarrassment to Texarkana College.

E. Storage of personal email messages, voice messages, files and documents within the College's Information Resources must be nominal.

All messages, files and documents – including personal messages, files and documents – located on College Information Resources are owned by the State of Texas, may be subject to open records requests and may be accessed in accordance with this agreement and any other applicable College policy or agreement.

Texarkana College Information Security Agreement

I understand and agree that I will be violating Texarkana College Administrative Procedures (Information Security), State Laws (Chapter 33, Section 1, Title 7 of the Texas Penal Code) and Federal Laws (Family Education Rights and Privacy Act of 1974 and Health Insurance Portability and Accountability Act of 1996) if I do not adhere to the provisions of this agreement.

I understand and agree that I do not possess the authority to grant anyone the use of my ID(s) and password(s) and that I am personally accountable for all actions that occur with the use of my ID(s). I understand that unauthorized access includes providing my ID(s) and password(s) to any other person. No other person may perform duties (as me or to assist me) where they must use my ID(s) and password(s). Authorized users violate this agreement when they receive and use any other user's ID(s) and password(s).

I understand and agree that I must secure access to any device in which I am logged into when I leave the vicinity of that device. I understand that securing access to a device includes logging out of or locking the device so that a password is required to regain access. Authorized users violate this agreement when they leave any device in which they are logged into without logging out or locking that device.

I understand and agree that Texarkana College information resources include:

A. Any college-wide applications to include the college's Enterprise Resource Program and associated systems and data, Active Directory data, the college email system, etc.
B. Client/Server-oriented applications and services;
C. Data warehoused reports retained by the college, on any media;
D. Client/server-oriented databases and file systems and the institutional data contained in them; and
E. Any desktop/laptops or other mobile devices or removable storage and the institutional data contained in them.

I understand and agree that accessing any other agency's systems, applications, and information through the Texarkana College information resources is subject to this agreement AND the administrative procedures, rules, and regulations of the accessed agency. **I understand and agree that I will only view those records for which I have a legitimate educational or business interest**.

I acknowledge my responsibility for adhering to U. S. Copyright law as expressed in System Regulation 21.99.10 regarding the use of licensed commercial software. I realize that my failure to do so may result in disciplinary action, prosecution, and a fine of up to $100,000.

I acknowledge that the destruction, removal, or alteration of public information or the distribution of confidential information are criminal violations included in Chapter 552, Subchapter 1 of the Texas Government Code. Violations may result in disciplinary action, prosecution with a maximum fine of $4,000 and up to six (6) months in jail. (See System Regulation 61.01.02 – Public Information)

I do hereby accept full responsibility for my actions as an authorized user of Texarkana College information resources and I will obtain proper authorization to access any other agency's information resources. I am also responsible for obtaining and reading any and all applicable administrative procedures, regulations, and laws referenced in this agreement.

Texarkana College Confidential Information Agreement

All Texarkana College employees with access to records, documents, and information which contain sensitive or confidential information are responsible for maintaining the integrity and confidentiality of those records. As an employee of Texarkana College you agree to and acknowledge:

A. During the course of your employment with the college you may be exposed to certain sensitive, confidential, personal, or proprietary information concerning the institution, students, or vendors consisting of:

1. Technical information including inventions, computer programs and research projects;
2. Business information including admissions data, financial information, governmental reports, reorganization plans, employee lists, plans for expansion, vendor information, organizational goals, fees data, sources of supply, marketing, educational, and instructional systems or plans; and
3. Personal information including but not limited to salary information, educational information, employment information, health or insurance information, payroll information, names, personal addresses, personal telephone numbers, personal email addresses, and social security numbers.

B. During your employment or any time after the termination of your employment with Texarkana College, you will not make use of or disclose to others any proprietary, sensitive personal information, confidential information, or any other data obtained as an employee of the college in violation of this agreement.

C. Upon termination of employment with Texarkana College you will:
   1. Return to Texarkana College all documents including but not limited to payroll, salary, employment information, student records, employee lists, reports, manuals, correspondence – including email correspondence, computer programs, and any other college related data; and
   2. Not delete or destroy business records, correspondence, or emails related to Texarkana College.

Texarkana College Photo, Video, Voice Recording, and Print Media Consent

In the course of your employment with Texarkana College, there may be occasions where your photograph, video image, voice recording, or other event may be captured on video, film, digital, or printed media. Signing the Information Technology agreement grants Texarkana College and its assignees the right to use those and similar media for college related purposes. By signing the agreement, you waive any and all claims you might otherwise have against Texarkana College or its assignees that may arise out of the use of such images and recordings.

Computer Equipment, Access to Programs, Systems, and Additions to Mailing Lists

Once you are established in the Human Resources Information System as an employee, you are then assigned an email account and access to system resources required for your job assignment. You may also be placed on selected mailing lists to receive group delivery of information pertaining to your job. Creation of your record in the HR system may take a few days based on caseload.

Once you are entered into the system as an employee, problems regarding computer system access, email, etc. should be directed to your supervisor or the Information Technology staff. Your supervisor is responsible for making arrangements to obtain the equipment and resources necessary to do your job. You and your supervisor will work closely with Information Technology to configure your level of access, services, and equipment.

Information Technology offices are located in the Aikin Building on the main campus. IT may be reached by phone at 903-823-3105. Work orders may be submitted via the web at https://www.texarkanacollege.edu/helpdesk or emailed to helpdesk@texarkanacollege.edu.

Information Technology Agreement (5 pages) signed and agreed to by:

Full Name (print clearly) _____ Title _____

Signature _____ Date _____

Division/Department _____

For IT Department Use Only
Security Administrator
Date

Appendix B

Acceptable Use

Texarkana College

Last Edited November 17, 2014

Introduction

Under the provisions of the Information Resources Management Act, Texas Gov. Code Chapter 2054, Information Resources are strategic assets of the State of Texas that must be managed as valuable state resources. Thus, this agreement is established to achieve the following:

A. To ensure compliance with applicable statutes, regulations, and mandates regarding the management of information resources;
B. To establish prudent and acceptable practices regarding the use of information resources; and
C. To educate individuals who may use information resources with respect to their responsibilities associated with such use.

Application of Agreement

The Acceptable Use Agreement applies equally to all individuals granted access privileges to any College Information Resources, including students and guests.

Ownership of Electronic Files

Electronic files created, sent, received, or stored on Information Resources owned, leased administered, or otherwise under the custody and control of the College are the property of the College and the State of Texas.

Privacy

Electronic files created, sent, received, or stored on Information Resources owned, leased, administered, or otherwise under the custody and control of College are not private and may be accessed by Information Technology employees at any time without the knowledge of or notice of Information Resources user or owner. Electronic file content may be accessed by appropriate personnel in accordance with the provisions and safeguards provided in the Texas Administrative Code 202, Information Resource Standards.

Protocol

A. Users must report any weaknesses in College computer security, any incidents of possible misuse, or any violation of this agreement to the CIO and other College officials as appropriate.
B. Users must not attempt to access any data or programs contained on College systems for which they do not have authorization or explicit consent.
C. Users must not share their College account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes.
D. Users must not make unauthorized copies of copyrighted software.
E. Users must not use non-standard shareware or freeware software without IT approval unless it is on the College standard software list.
F. Users must not:
    1. Purposely engage in activity that may harass, threaten or abuse others;
    2. Deprive an authorized College user access to a College resource;
    3. Obtain extra resources beyond those allocated, or;
    4. Circumvent College computer security measures.

G. Users must not download, install or run security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, College users must not run password cracking programs, packet sniffers, or port scanners or any other non-approved programs on College Information Resources.
H. College Information Resources must not be used for personal benefit.
I. Users must not intentionally access, create, store or transmit material that the College may deem to be offensive, indecent or obscene (other than in the course of academic research where this aspect of the research has the explicit approval of the College's official processes for dealing with academic ethical issues).
J. Access to the Internet from a College-owned, home-based, computer must adhere to all the same policies that apply to use from within College facilities. Users must not allow family members or other non-employees to access College computer systems.
K. Access to the College network from a personally-owned, home-based, computer or other device must adhere to all the same policies that apply to use from within College facilities. Users must not allow family members or other non-employees to access College computer systems.
L. Users must not otherwise engage in acts against the aims and purposes of the College as specified in its governing documents or in rules, regulations and procedures adopted from time to time.

Incidental Use

As a convenience to the College user community, incidental use of Information Resources is permitted with the following restrictions:

M. Incidental personal use of electronic mail, internet access, fax machines, printers, copiers, etc., is restricted to College approved users; it does not extend to family members or acquaintances.
N. Incidental use must not result in direct costs to Texarkana College.
O. Incidental use must not interfere with the normal performance of an employee's work duties.
P. No files or documents may be sent or received that may cause legal action against, or embarrassment to Texarkana College.
Q. Storage of personal email messages, voice messages, files and documents within the College's Information Resources must be nominal.

All messages, files and documents – including personal messages, files and documents – located on College Information Resources are owned by the State of Texas, may be subject to open records requests and may be accessed in accordance with this agreement and any other applicable College policy or agreement.

Appendix C

Access, Security and Control of Data and Information

Texarkana College

Last Edited November 17, 2014

Purpose

The purpose of this document is to establish practices and procedures for the protection of the College computerized information systems, data, and software and to establish rights and responsibilities for the protection of staff, faculty, and students who use these information systems.

Scope

Practices and procedures defined in this document apply to students, faculty members, officers and employees of Texarkana College, as well as contractors, consultants, vendors and all others granted use of and/or access to TC data and technology resources.

Protocol

Data contained in the College's systems are the property of TC and represent official College records. Users who accept access to this data, whether on-line or in datasets, also accept responsibility for adhering to certain principles in the use and protection of that data:

- Information systems within the College shall be used only for and contain only data necessary for fulfillment of the College's mission.
- College data shall be used solely for the legitimate business of the College.
- Due care shall be exercised to protect College data and information systems from unauthorized use, disclosure, alteration or destruction.
- College data, regardless of who collects or maintains it, shall be shared among those faculty or staff whose responsibilities require knowledge of such data.
- Applicable federal and state laws (i.e. the Privacy Act), and College policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate College procedures shall be followed in reporting any breach of security or compromise of safeguards.
- College computerized information systems shall be constructed in such a manner to assure that:
    - Accuracy and completeness of all system contents are maintained during storage and processing;
    - Data, text and software stored and processed can be traced forward and backward for audit ability;
    - Information systems capabilities can be re-established within an acceptable time upon loss or damage by accident, malfunction, breach of security or act of God; and
    - Actual or attempted breaches of security can be detected promptly.
- Any faculty, staff member, or student engaging in unauthorized use, disclosure, alteration, or destruction of information systems or data shall be subject to appropriate disciplinary action, including possible dismissal.
- Users may not use, query, release or print data in any application which they have not been given deliberate access to, which can include, but is not limited to:
    - Transcripts, grade reports, enrollment reports;
    - Financial Aid information;
    - Personnel, leave, salary reports;

- Reports for government or funding agencies;
- Fund-raising activities;
- Mailing lists and labels;
- Private or public release of data to outside parties such as students, parents and the news media.

Responsibilities

Safeguarding of College information systems and data shall be the responsibility of each faculty or staff member with knowledge of the system or data. Specific responsibilities are as follows:

- Management – all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined in this document. Specifically, managers are responsible for validating the access requirements of their staff according to their job functions, prior to submitting requests for the provision of access, and for ensuring a secure office environment with regard to College information systems. Managers of major College offices should appoint an individual within their staff to ensure these responsibilities are observed.
- Users – are responsible for the protection, privacy, and control of all data, regardless of the data storage medium. Users must ensure that the data and data media are maintained and disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the user's administrative and academic duties. Users are responsible for all transactions occurring under his/her user ID and/or password. Passwords and user IDs may not be shared with anyone under any circumstances unless the CIO specifically approves an exception.
- CIO – is responsible for ensuring that appropriate security controls are being provided, including protection of all areas of risk or exposure.
- Information System Security Specialist – is responsible for providing administrative, technical and educational support in the area of information security for all users of administrative systems. This support includes, but is not limited to:
    - Creation and deletion of user IDs and/or account numbers, after appropriate approval has been obtained.
    - Providing access to administrative systems, transactions, or production after appropriate approval.
    - Recommendations to the CIO on appropriate training to ensure consistent practice among departmental support personnel.

Questions or Problems

Questions, concerns or additional information about this document or other IT related concerns should be directed to the CIO.

Responsibility

The Chief Information Officer (CIO) is the administrator for information technology resources and will ensure this process is followed. Additionally, Deans, Directors and Department Heads are responsible for compliance with the college's security program within their respective administrative areas.

Appendix D

Data Center Access

Texarkana College

Last Edited November 17, 2014

Purpose

To ensure security measures are in place to protect Information Technology's Data Centers.

Scope

This document applies to all College staff, faculty, administrators, officers and students (collectively, "users"), including those accessing systems and services remotely.

Data Center Access

- Shall only be authorized through a written request by the individual's Director to the CIO. This request must provide appropriate justification for access.

Data Center Access Rules

Individuals granted access to the Data Center are required to adhere to important policies and procedures such as:

- No food or drink of any type is permitted in the Data Center.
- The following policies shall be complied with while in the Data Center:
    - Acceptable Use of Information Technology Resources (Appendix B)
    - Access, Security and Control of Data and Information Practices and Procedures (Appendix C)
- The official and most recent version of the above documents can be found on the Texarkana College web site. It will be the individual's responsibility to visit the website and familiarize themselves with the most recent and official version of these documents.
- Access to the Data Center is controlled by access fobs. Individuals assigned a fob must keep it secure at all times. Under no circumstances are they to loan their access fob to another individual.
- Activities within the Data Centers shall be restricted, as much as is reasonably possible, to the area where the visitor's equipment and/or systems are stationed.
- If an unauthorized person is escorted into the Data Centers, the authorized visitor must remain with that person at all times while they are in the Data Centers.
- Access to the Data Center is monitored by cameras; therefore, the activities of all individuals in the Data Center shall be recorded.

Questions or Problems

- Call the Help Desk at 903-823-3030. Voice mail is available around the clock, 365 days a year. We will respond the next business day if you leave a message outside normal office hours.
- Email us at helpdesk@texarkanacollege.edu. Briefly describe the assistance you need, tell us the best time to contact you, and provide a phone number.

Responsibility

The Chief Information Officer (CIO) is the administrator for information technology resources and will ensure this process is followed. Additionally, Deans, Directors and Department Heads are responsible for compliance with College practices and procedures within their respective administrative areas.

Appendix E

Data Protection – Authorization Controls Standard

Texarkana College

Last Edited November 17, 2014

Purpose

The purpose of the Authorization Controls Standard is to provide guidance to those who are responsible for granting access to Texarkana College (TC) technology resources and data. The technology resources and data referred to in this standard include those owned by or entrusted to the College for the purpose of supporting academic, administrative, research or service related activities.

In addition to fulfilling the responsibility of effectively protecting data belonging to the College, as well as its customers and partners, users of the college's information systems are also subject to applicable external regulations, including but not limited to:

- Family Educational Rights & Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Federal Export Technology Control Laws
- The Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCIDSS)
- Sarbanes Oxley Act (SOX)

Scope

This Standard applies to students, faculty members, officers and employees of Texarkana College, as well as contractors, consultants, vendors and all others granted use of and/or access to TC data and technology resources.

Standard Statement

College entities with ownership and custodial responsibilities for operating and maintaining College applications/systems and data must implement formal procedures for granting, tracking and revoking access to data. With respect to technology resources, this authorization is typically implemented through the assignment of an electronic account, access card or other authentication mechanism. Authorization must be based on the least privilege and need to know principles according to an individual's job responsibilities. The authorization controls must include methods to collect and maintain the following records:

- Purpose for access to the resource or data
- Dates of authorization (initial and subsequent changes)
- Effective dates or duration of authorization
- Record of individual(s) authorizing the access
- Record of the individual(s) receiving the access privileges
- Type and scope of access privileges
- Procedures for tracking accounts and privileges based on responsibilities and employment status, including position changes or separation from the College

Security of Data

Although every effort is made to secure network communications, Texarkana College cannot ensure the privacy of online communications. Individuals using online services should also take steps to protect personal information, such as closing the web browser when finished using the site. Failure to do so may result in personal information being viewed by someone else using the same computer.

Texarkana College accepts credit card payments online for a variety of goods and services. Unless otherwise noted on the site, all Texarkana College credit card transactions are encrypted. Confidential information entered to complete a transaction will not be used by Texarkana College for any other purpose unless the purpose is described on the site.

Texarkana College maintains the right to examine College-owned computers and equipment to detect illegal software and to evaluate the security of the network.

Legal Standards

All Texarkana College Users are expected to abide by all Federal and State laws. The following list is used for illustrative purposes, and is not intended to be a comprehensive guide to Federal and/or State law:

- FERPA (Family Educational Rights and Privacy Act): regulates the confidentiality of student records.
- GLBA (Graham Leach Bliley Act): regulates the confidentiality of financial information.
- HIPAA (Health Insurance Portability and Accountability Act): regulations the security and privacy of heath information.
- PCI DSS (Payment Card Industry Data Security Standard): regulates the confidentiality of credit card information.
- DMCA 1998 (Digital Millennium Copyright Act): regulates the protection of intellectual property.
- USC Title 18 §1030 (United States Code): Fraud and related activity in connection with computers

Questions or Problems

Questions, concerns or additional information about this and other IT concerns should be directed to the CIO.

Responsibility

All members of the TC community are responsible for information security. Accordingly, all members are charged with providing full support to maintain this standard. It is the responsibility of the administrators of their respective areas to implement measures to achieve and maintain these standards within their college, department or unit.

Appendix F

Electronic Account Standards

Texarkana College

Last Edited November 17, 2014

Purpose

The purpose of the Electronic Account Standard is to provide a set of minimum operational and security related standards for electronic accounts that are used to identify individuals and authenticate access to Texarkana College (TC) data and technology resources. Generally, the electronic accounts used at TC consist of a username and password.

Electronic accounts are issued to students, faculty and employees for the purpose of conducting academic, research, service and/or administrative activities that support the College's mission. Periodically, other parties such as contractors, vendors, library patrons and guests are issued an electronic account for a limited period or purpose to support a College resource, use a service provided by the College or to participate in a College sponsored activity.

Scope

This Standard applies to students, faculty members, officers and employees of Texarkana College, as well as contractors, consultants, vendors and all others granted use of and/or access to TC data and technology resources.

Standards Electronic Accounts

- Authentication Requirements. Technology resources (e.g., computers, laptops, applications and systems) that produce, maintain, transmit or permit access to College data or data entrusted to the College must be protected, at minimum, by an electronic account or other approved authentication mechanisms.
- Unique Accounts or Authentication Mechanisms. Each individual granted access to TC resources will be assigned his or her own unique electronic account(s) or authentication mechanism(s) for the purpose of accessing and using authorized information and/or resources. Except for the departmental accounts, discussed below, sharing of accounts is prohibited.
- Departmental/System Accounts. Departmental accounts are accounts shared by multiple, but individually authorized individuals for a specific purpose, such as managing a departmental electronic mail account, system files and structures, or a computer that must operate in a continuous processing state. An account manager must be identified for each departmental or system account.
- Guest Accounts. Guest accounts may be provided to allow temporary access to College resources for a specific purpose and period. The parties authorizing and issuing the guest accounts must establish formal authentication, accountability and tracking procedures. All guest accounts must be created with an expiration date and time. Guest accounts must be disabled immediately upon the expiration date.
- Initial Delivery and Resets of Electronic Accounts and Authentication Mechanisms. An initial or reset password will be established or re-established using a unique, randomly generated password.
- Inactive Account Expiration. An expiration date, of 90 days or less from the account activation date, must be established when setting up an account. Expired accounts must be locked, disabled or otherwise protected from unauthorized access.

Passwords and Usernames

- Periodic Password Changes. Systems must require users to change their passwords once every 90 days.
- Password Reuse. Systems shall include controls that prevent reuse of passwords during a 365-day cycle.
- Password Composition. Passwords shall be at least eight (8) characters in length and 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 Lockout. Systems that maintain or allow access to resources that house confidential, or business-limited information shall implement account lockout mechanisms, with the maximum failure limit set to five (5) attempts in order to minimize the risk that an unauthorized party will gain access to a resource using brute force or random, persistent guessing.
- Compromised Accounts. 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.
- Password Capture. Passwords shall be masked during capture or keyboard entry.
- Password Storage and Transmission. All stored passwords will be encrypted.
- Different Username and Password. Authentication mechanism consisting of a user name and password shall require a password that is different from the user name. Blank usernames or passwords shall not be permitted.
- Authorization to use Existing Authentication Credentials, Usernames and Passwords. Before using existing authentication credentials, one must obtain authorization from the entity that manages the credentials.

Questions or Problems

Questions, concerns or additional information about this and any IT protocol should be directed to the CIO office.

Responsibility

As described in the Information Security Program, all members of the TC community are responsible for information security. Accordingly, all members are charged with providing full support to maintain this standard. It is the responsibility of the Dean or Director to implement measures to achieve and maintain these standards within their college, department or unit.