The University of Texas Permian Basin

Information Security Policies

Table of Contents

Contents

1. Information Security Program

1.1 The Information Security Office (ISO) at The University of Texas Permian Basin (UTPB) establishes these Information Security Policies to protect the confidentiality, integrity, and availability of information resources of UTPB.

1.2 This document applies equally to all personnel including, but not limited to: management, employees, agents, consultants, volunteers, students, and any other users of UTPB Information Resources.

1.3 ISO will reduce the collection, use, and protect from disclosure social security numbers (SSNs) and Credit Card Numbers (CCNs) in all forms across UTPB.

1.4 Title 1 Texas Administrative Code 202.70(1) states that it is the policy of the State of Texas that Information Resources residing in the various institutions of higher education of state government are strategic and vital assets belonging to the people of Texas. Assets of UT System must be available and protected commensurate with their value and must be administered in conformance with federal and State law and the U. T. System Regents' Rules and Regulations. This Policy provides requirements and guidelines to establish accountability and prudent and acceptable practices regarding the use and safeguarding of the UTPB Information Resources, to protect the privacy of personally identifiable information contained in the data that constitutes part of its Information Resources, to ensure compliance with applicable policies and State and federal laws regarding the management and security of Information Resources, and to educate individual users with respect to the responsibilities associated with use of UTPB Information Resources.

1.5 This policy is based off of UTS-165, TAC 202, and FERPA regulations.

1.6 Certain portions of UTPB's Information Security program may be considered confidential under Texas Government Code Section 552.139. Any section of the Information Security program determined by the UTPB Chief Information Security Officer (CISO) to be confidential will be redacted before public release.

1.7 This policy will be reviewed, and if needed, updated at last annually by the CISO.

2. Acceptable Use Policy

2.1 The Acceptable Use Policy (AUP) approved by the Office of General Council (OGC) applies to UTPB. It can be found at: Acceptable Use Policy.pdf

3. Information Security Standards Violations

3.1 UTPB will protect the Information Resources assets of the state of Texas in accordance with the state of Texas Department of Information Resources' (DIR) Information Resources Security and Risk Management Policy, and Guidelines as published in the Texas Administrative Code 1 TAC 202, as authorized by the Information Resources Management Act (Chapter 2054, Texas Government Code Annotated), and in compliance with UTS-165.

Specifically, UTPB will apply policies, procedures, practice standards, and guidelines to protect its Information Technology functions from internal data or programming errors and from misuse by individuals within or outside the University. This is to protect UTPB from the risk of compromising the integrity of State programs, violating individual rights to privacy and confidentiality, violating criminal law, or potentially endangering the public's safety.

All UTPB Information Technology security programs will be responsive and adaptable to changing technologies affecting Information Resources.

3.2 Any event that results in theft, loss, unauthorized use, unauthorized disclosure, unauthorized modification, unauthorized destruction, or degraded or denied services of IR constitutes a breach of security, confidentiality, availability, and integrity. Violations may include, but are not limited to any act that:

a. Makes available information to any individual to which authorization was not given by ITS.
b. Exposes the agency to actual or potential monetary loss through the compromise of Information Resources security,
c. Involves the possibility of disclosure of sensitive or confidential information or the unauthorized use of agency data or resources,
d. Involves the use of Information Resources for personal gain, unethical, harmful, or illicit purposes, or results in public embarrassment to the agency.

3.3 Violation of these Policy Standards may result in immediate disciplinary action that may include, but may not be limited to:

a. Counsel with the CISO
b. Formal reprimand
c. Suspended or restricted access to agency Information Resources
d. Restitution or reimbursement for any damage or misappropriation of any agency property

e. Suspension without pay
f. Termination of employment
g. Termination of contract
h. Expulsion (permanent separation from the institution, as imposed by the Student Affairs Officer if applicable)
i. Civil prosecution, or state and/or federal criminal prosecution.

4. Changes and Approval Process

4.1 The Information Security Office (ISO) Information Security Policies are based on laws, regulations, and industry standard best practices. ISO Information Security Policies will be drafted and proposed by the CISO, as needed to maintain compliance. The proposals will be approved by the Vice President for Business Affairs and the President.

5. Physical Security Plan

5.1 The Physical Security Plan is intended to provide reasonable protection for a portion of the institution's information resource assets. This plan addresses physical security for specific agency information assets. The plan is limited in scope to information assets over which the UTPB Information Technology Services has been assigned custodial responsibilities.

Any valid security plan must start by addressing physical security. Without adequate physical security, logical security controls are ineffective. Information resource assets cannot be logically secured against an attacker if the attacker has physical access to the resources. Furthermore, only through adequate physical security can the loss of equipment and components through theft be minimized. The physical security plan seeks to achieve a balance between adequate security and acceptable utility.

5.2 Zone Definitions:

5.2.1 Red Zone – Secure Area

The Red Zone represents space with the most rigorous physical security requirements. This space will be referred to as Secure Area. Security requirements include both physical and administrative elements. Security requirements for this zone arise due to the large concentration of mission-critical equipment in the space, the presence of confidential data in the space, and the high density and special nature of network connections within the space. The space has the following security requirements:

a. Normal access to this space is limited to designated full-time ITS employees and the CISO.
b. Non-ITS employees with legitimate needs to be within the space must sign a written log upon entry and exit and must be accompanied by a full-time ITS employee while in the space.
c. This space is off-limits to the general public, the general student population, and hourly (part time) ITS employees. All other university employees are prohibited from the area unless a specific reason for entry exists (maintenance, cleaning, etc.) or an emergency situation exists. University

employees that are not ITS personnel will be escorted in the space during non-emergency routine access.

d. All doors into this space are to be closed and locked at all times.
e. Major access points will be monitored by a key-card system capable of uniquely identifying the entry point, date, time and access card used for entry.
f. The space will be continuously monitored for temperature, power status, subfloor moisture, ambient noise and smoke. When any monitored variable exceeds an established set point, automatic notification procedures will be initiated.
g. The space will be protected by a self-contained fire detection and suppression system.
h. Each door into the Red Zone will be marked with a placard that reads "Secure Area, ITS Personnel Only".

5.2.2 Blue Zone – Restricted Area

The Blue Zone represents space with an intermediate physical security requirement. These requirements are intended primarily to protect state-owned information assets from pilferage and theft. These requirements also arise due to the potential presence of sensitive information within the zone. This zone has the following security requirements:

a. Normal access to this space is limited to full-time and hourly ITS employees.
b. University employees with legitimate needs to be within the space must be cleared through the appropriate access point and exit through the same point.
c. This space is off-limits to the general public and to the general student population.
d. All doors into this space are to be closed and locked at all times. Doors to this area will have security considerations in their design (i.e. hinge type, windows, locks, etc.)
e. Major access points will be monitored by an access code lock system capable of uniquely identifying the entry point, date, time and entry code used for access.
f. Each door into the Blue Zone will be marked with a placard that reads "Restricted Area, Authorized Personnel Only".

5.3 In addition to the zones defined in section 5.2, a secure perimeter is defined for the primary information resource support area. This perimeter identifies doors to which special security monitoring applies. Taken collectively, security monitoring on defined perimeter doors should be configured so as to provide notification to the central security monitoring station in the event a perimeter door is opened after the perimeter security monitoring system has been enabled.

UT Permian Basin
Information Security Office
Information Security Policies

6. Security Responsibilities

6.1 Owners, custodians, and users of information resources shall be identified, and their responsibilities defined and documented by the institution of higher education. In cases where information resources are used by more than one major business function, the owners shall reach consensus and advise the ISO as to the designated owner with responsibility for the information resources. The following distinctions among owner, custodian, and user responsibilities should guide determination of these roles:

6.1.1 Owner Responsibilities: The owner or his or her designated representatives are responsible for and authorized to:

a. Approve access and formally assign custody of an information resources asset
b. Determine the asset's value
c. Define, approve, and document acceptable risk levels and risk mitigation strategies.
d. Conduct and document risk assessments to determine risk and inherent impact that could result from unauthorized access, use, disclosure, disruption, modification, or destruction.
e. Specify data control requirements and convey them to users and custodians.
f. Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the institution of higher education.
g. Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data
h. Ensure compliance with applicable controls.
i. Assign custody of information resource assets and provide appropriate authority to implement security controls and procedures.
j. Review access lists based on documented security risk management decisions.
k. Adopt a disaster recovery plan commensurate with the risk and value of the information resource and data. The disaster recovery plan must incorporate procedures for recovering data and applications.

6.1.2 Custodian Responsibilities: Custodians of information resources, including entities providing outsourced information resources services to state institutions of higher education must:

a. Implement the controls specified by the owners.
b. Implement approved Risk mitigation strategies and adhere to Information Security Policies and Procedures to manage risk levels for Information Resources under their care.
c. Provide physical and procedural safeguards for the information resources

d. Assist owners in evaluating the cost-effectiveness of controls and monitoring
e. Implement the monitoring techniques and procedures for detecting, reporting, and investigating incidents.

6.1.3 User Responsibilities: Users of information resources shall use the resources only for defined purposes and comply with established controls.

7. Security Policy Standards

7.1 Information Resource controls must not be bypassed or disabled.

7.2 Security awareness of personnel must be continually emphasized, reinforced, updated, and validated.

7.3 All personnel are responsible for managing their use of Information Resources and are accountable for their actions relating to Information Security. Personnel are also equally responsible for reporting any suspected or confirmed violations of this policy to the appropriate management.

7.4 Passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcards, One Time Passwords), and other computer systems, security procedures and devices shall be protected by the individual user from use by, or disclosure to, any other individual or organization. All security violations shall be reported to the custodian or owner department management and the CISO.

7.5 Access to, change to, and use of Information Resources must be strictly secured. Information access authority for each user must be reviewed on a regular basis, as well as each job status change such as: a transfer, promotion, demotion, or termination of service. User access to applications and data is granted on a need-to-access basis.

7.6 The use of Information Resources must be for officially authorized business purposes only. There is no guarantee of personal privacy or access to tools such as, but not limited to: email, Web browsing, and other electronic discussion tools. The use of these electronic communications tools may be monitored to fulfill compliance or investigation requirements. Departments responsible for the custody and operation of computers (custodian departments) shall be responsible for proper authorization of Information Resource utilization, the establishment of effective use, and reporting of performance to management.

7.7 Any data use in an IT system must be kept confidential and secure by the user. The fact that the data may be stored electronically does not change the requirement to keep the information confidential and secure. Rather, the type of information or the information itself is the basis for determining whether the data must be kept confidential and

secure. Furthermore, if this data is stored in a paper or electronic format, or if the data is copied, printed, or electronically transmitted the data must still be protected as confidential and secured.

7.8 On termination of the relationship with the agency users must surrender all property and IR managed by the agency. All security policies for IR apply to and remain in force in the event of a terminated relationship until such surrender is made. Further, this policy survives the terminated relationship.

7.9 The owner must engage the IRM, or designate, at the onset of any project to acquire computer hardware or to purchase or develop computer software. The costs of acquisitions, development, and operation of computer hardware and applications must be authorized by appropriate management. All hardware and software purchases and renewals must also be approved by the IRM and the ISO. Use of unauthorized or unapproved software is prohibited. Management and the requesting department must act within their delegated approval limits in accordance with the agency authorization policy. A list of standard software and hardware that may be obtained without specific individual approval has been published.

7.10 The department which requests and authorizes a computer application (the owner) must take the appropriate steps to ensure the integrity and security of all programs and data files created by, or acquired for, computer applications. To ensure a proper segregation of duties, owner responsibilities cannot be delegated to the custodian.

7.11 The IR network is owned and controlled by ITS. Approval must be obtained from ITS before connecting any device to the network. ITS and the ISO reserves the right to remove any network device that does not comply with standards or is not considered to be adequately secured.

7.12 The sale or release of computer programs or data, including email lists and departmental telephone directories, to other persons or organizations must comply with all agency legal and fiscal policies and procedures.

7.13 The integrity of general use software, utilities, operating systems, networks and respective data files are the responsibility of the custodian department. Data for test and research purposes must be depersonalized prior to release to testers unless each individual involved in the testing has authorized access to the data.

7.14 All changes or modifications to IR systems, networks, programs or data must be approved by the owner department that is responsible for their integrity.

7.15 Custodian departments must provide adequate access controls in order to monitor systems to protect data and programs from misuses in accordance with the needs defined by owner departments. Access must be properly documented, authorized, and controlled.

7.16 All computer systems contracts, leases, licenses, consulting arrangements or other agreements must be authorized and signed by an authorized agency officer and must contain terms approved as to form by the UT System Office of General Counsel, advising vendors of the agency's IR retained proprietary rights and acquired rights with respect to its information systems, programs, and data requirements for computer systems security, including data maintenance and return. Software is to be used in accordance with the applicable licensing agreement. Unauthorized or unlicensed use of software is prohibited and subjects the User to disciplinary action. Any unauthorized or unlicensed use is deemed to be without the consent of UTPB.

7.17 IR computer systems and/or associated equipment used for agency business that is conducted and managed outside of agency control must meet contractual requirements and be subject to monitoring.

7.18 External access to and from IR must meet appropriate published agency security guidelines.

7.19 All commercial software used on computer systems must be supported by a software license agreement that specifically describes the usage rights and restrictions of the product. Personnel must abide by all license agreements and must not illegally copy licensed software. ITS reserves the right to remove any unlicensed software from any computer system.

7.20 ITS reserves the right to remove any non-business related software or files from any system. Examples of non-business related software or files include, but are not limited to; games, instant messengers, pop email, music files, image files, freeware, and shareware.

7.21 Use of information resources should only be used for purposes of fulfilling UTPB mission-related duties. Network traffic and use of information resources is monitored as authorized by applicable law.

7.22 Adherence to all other policies, practice standards, procedures, and guidelines issued in support of these policy statements is mandatory.

8. **User Security Practices**

8.1 Section 8 provides a list of required security practices for users of UTPB Information Resources. These practices are designed to reduce the number of malware and virus infections and also the number of compromised accounts.

8.2 Do not open any files attached to an email from an unknown, suspicious, or untrustworthy source.

8.3 Do not open any file attached to an email unless you know what it is, even if it appears to come from a dear friend or someone you know. Some viruses can replicate themselves and spread through email. The safest approach is to confirm that the apparent sender really sent the message/attachment.

8.4 Do not open any files attached to an email if the subject line is questionable or unexpected.

8.5 Do not use e-mail attachments unless your message really needs an attachment. For example, if your message consists of only plain text, send the message as a plain text message, not as a Word attachment. This approach is much more efficient and eliminates the potential for an infected attachment. Use attachments only when necessary and keep message size as small as possible.

8.6 Do not use 3rd party "enhancements" to your e-mails, eg. special backgrounds and special signature blocks. These items contribute little to the utility of your message, needlessly increase the size of your message and represent potential virus infection or security problems. Simple text messages are the most efficient and least likely to provide an infection path for virus activity.

8.7 Delete chain emails and junk email. Do not forward or reply to them. This type of email is called "spam", which is unsolicited, intrusive mail that slows down the network. Responding will only result in more junk mail. Be careful about entering your email address in Web sites that require you to register in order to access the features available on the Web site. Some sites will sell your email address to spammers. You may want to read the site's privacy statement before submitting your information.

8.8 Be sure that you understand University rules, state laws and federal laws governing the sending of Unsolicited Bulk E-Mail (UBE) BEFORE you consider using any form of mass e-mail facility. State and federal law now place specific requirements and restrictions on UBE senders.

8.9 Use of unapproved utilities is prohibited. This includes custom screen savers, special backgrounds, special cursors, special tool bars, performance "enhancers", or any other bloatware. While some of these "free" applications may appear to offer attractive functionality, many of these items are of questionable origin and almost all of them rob your system of performance. Some may represent serious security threats to the university network.

8.10 Update your anti-virus software regularly. Most anti-virus software consists of two components; the scan engine and the virus definitions. Since the virus world is very

dynamic, the virus definitions should be updated frequently. Most University systems are configured to do this update automatically. The specifics of how this is done depend on the particular anti-virus software being used.

8.11 Do not share passwords. The UTPB Acceptable Use Policy requires that all passwords be used only by the assigned account holder. Do not divulge your passwords to anyone. Never provide your password to someone over the telephone, even if they claim to be "From IT".

8.12 All system data, including data associated with research, must be backed up in accordance with risk management decisions implemented by the Data Owner. End-user files and research data should be saved or backed up to a location other than the local computer. ITS approved locations are OneDrive, Sharepoint, Teams, or to a network share.

8.13 UTPB requires all staff to have an electronic device for mandatory Multi-Factor Authentication (MFA) when accessing University systems. This policy aims to enhance the security of digital infrastructure. Staff members must possess an electronic device capable of receiving MFA authentication codes, such as smartphones, tablets, or hardware tokens. Approved MFA methods include authenticator apps, SMS/text messages, phone calls, or hardware tokens. It is the responsibility of each staff member to secure their device, and non-compliance may result in restricted system access. The University's IT department will provide support for enrollment and troubleshooting, ensuring a secure digital environment.

9. **Security Training Standards**

9.1 Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving UTPB's security goals. This can be accomplished with a combination of general computer security awareness training and targeted, product-specific training. The philosophy of protection and specific security instructions needs to be taught to, and re-enforced with, computer users. The security awareness and training information needs to be continuously updated and reinforced.

9.2 All new users must complete an approved Information Security Awareness course prior to being granted access to any UTPB information resources.

9.3 All users must sign an acknowledgement stating they have read and understand UTPB requirements regarding computer security policies and procedures.

9.4 All users (employees, consultants, contractors, temporaries, etc.) must be provided with sufficient training and supporting reference materials to allow them to properly protect UTPB information resources.

9.5 The ISO must maintain and distribute UTPB information security policies and procedures.

9.6 All users must successfully complete an annual computer security compliance course.

9.7 The ISO must develop and maintain a communications process to be able to communicate new computer security program information, security bulletin information, and security items of interest.

10. Password Guidelines

10.1 Passwords are the primary method to identify and authenticate users to information resources. Two-factor authentication will also be required in certain situations, as determined by Information Security and ITS.

10.2 Passwords must meet the following minimum requirements as supported by the system:

a. Contain at least 12 characters.
b. Must not contain repetitive or sequential strings, such as:
    i. 1234567890asdf
    ii. 11111222223333310.2.3
c. The password must NOT be any of the following:
    i. A derivative of the username
    ii. A 12-letter word found in a dictionary (English or foreign)
    iii. Commonly used passphrases
    iv. Other simple words or patterns that hackers are likely to guess

10.3 Passwords must be changed by the user in an interval not to exceed 365 days.

10.4 Passwords will be changed anytime there is suspicion that a user's account has been accessed by any person other than the authorized individual. If repeated attempts to authenticate a user account fail, a password change may be required with increased complexity requirements at the discretion of the CISO (i.e. Brute Forcing Attempts).

10.4.1 The CISO will disable or suspend any user account at his or her discretion to maintain security of UTPB Information Resources.

10.5 The basis for password strength is the number of character combinations in any given length and the number of guesses per second that modern hardware is capable of computing. As hardware improves with time, password strength should match this improvement in computing power to prevent an attacker from guessing a user's password. The CISO will review password policies on a yearly basis.

10.6 Password guidelines:

10.6.1 Do not use an easily guessed password. Some examples of passwords that are easy to guess:

a. Names of family, pets, friends, co-workers, etc.
b. Computer terms, names, commands, sites, companies, hardware, software.
c. Birthdays and other personal information
d. Word or number patters (i.e. aaabbb, qwerty, zyxwvuts, 123321, etc.)

10.6.2 Passwords should never be stored on-line, for example, in an email addressed to yourself or in an Office document.

10.6.3 Handwriting passwords on paper and storing them within physical access of a workstation (i.e. under the keyboard or on the monitor) is prohibited.

10.6.4 Different passwords will be used for every system. This prevents an attacker from accessing multiple systems with the discovery of one password.

10.6.5 Use of an encrypted password vault is encouraged where feasible, provided the database and key file to that database are kept separate and secure. The use of password vaults typically contributes to a more secure, complex password that does not require memorization.

10.7 If a particular system does not support these minimum standards, the strongest password that system supports will be used.

10.8 Disclosure of a user's password, either inadvertent or intentional, to any person, for any reason, by anyone (including the authorized individual) except issuance to the individual by ITS, is strictly forbidden. Violation is subject to disciplinary action in accordance with section 3. Upon discovery by any individual that this has taken place, inform the CISO promptly.

10.9 Unattended computing devices will be protected from unauthorized access that could result from password guessing or idle session access with controls such as maximum login attempt lockouts and password-protected, locking screens.

11. **User Account Management**

11.1 Account requests for faculty, staff, and affiliates must originate with an authorized account sponsor. Usually the account sponsor will be a full-time employee with supervisory authority over the individual for whom an account is being requested. The account sponsor will document authorization for a new user account through the submission of a User Account Registration form (UAR) to ITS. The UAR will indicate the name of the individual to whom the account will be assigned. Every user account must be assigned to a unique, responsible individual. Generic, or shared user accounts are not permitted.

11.2 Data access rights are determined by data owners and implemented as a part of the account creation process. Data access rights are granted by data owners based on user roles or on individual assignments. Generic access rights for standard institutional roles will be maintained by the ISO and/or ITS.

11.3 Upon receipt of a properly completed UAR, UTPB ITS will initiate the creation of the requested user accounts.

11.4 Once the user account has been assigned the requested permissions, ITS will issue the login credentials to the user. Login credentials may not be given to anyone other than the verified user. ITS may verify the user via the following means:

a. Driver's license from the United States or Canada
b. U.S. or foreign passport
c. UTPB Identification card
d. Alien registration card with photo (INS form I-151 or I-551)
e. U.S. citizen ID card (INS form I-197)
f. Resident citizen card (INS form I-179)

11.5 Employee accounts will be terminated as soon as practical after the employee's last scheduled employment day. In situations where an employee is otherwise terminated, account terminations will be documented through the submission of a service request and will be implemented as soon as practical after ITS receives notice of the termination.

11.6 Student accounts will be initially created when the student applies. Accounts for students who withdraw from the University stay active in the event they re-enroll the following semester. If they do not re-enroll the following semester, the account is deactivated.

11.7 At least annually, all active user accounts will be compared against the best available list of current employees.

11.8 Guest accounts are generally not issued, except for special circumstances when approved by the CISO. For example, situations such as temporary contractors, Persons of Interest (POI's) requiring access, large groups needing short-term temporary access. Guest account requests originate from a supervisor role. Users with permanent accounts are prohibited from using a guest account. Guest accounts must be set to expire after a fixed amount of time, appropriate for the situation.

12. **Institutional Data Classification**

12.1 UTPB will classify data based on Section 9.5 of UTS-165.

12.2 Data classification levels can be found on the Data Classification Standard.

13. **Server Management Standards**

13.1 The owner of a server is responsible for the management, operation and security of the server. At a minimum, the owner must assure that University servers are physically secured, that electronic access to University servers is properly controlled, that University server configurations are maintained within specific security parameters and that adequate failure recovery practices are followed. The owner may delegate management responsibility for the server to a custodian or technical manager. The assigned custodian or technical manager is responsible for the actions of both the server and server users. The owner of a server may elect to impose additional requirements beyond the scope of this policy to achieve mandated regulatory compliance or to protect any designated private, confidential, sensitive, or otherwise protected information maintained or archived in the server.

13.2 General responsibilities regarding University server management are outlined below:

a. Owner: The owner must insure that anyone assigned to manage a server is qualified to perform technical duties, has adequate back up and receives resources necessary, including appropriate training or instruction, to comply with the requirements of this and other policies.

b. Custodian: The custodian administers, controls and configures servers in compliance with the requirements of the owner and policies in force.

c. Technical Manager: The technical manager is assigned by the resource owner or custodian to manage server(s). The assigned technical manager shall maintain knowledge and expertise equivalent to the scope of assigned responsibilities and systems supported.

13.3 Server Management Requirements

13.3.1 Environmental

a. University servers must be maintained in a physically secure location. Physical access to the equipment must be limited to a documented list of authorized individuals.
b. University servers must be protected by an Uninterruptable Power System with sufficient reserve run time to conduct an orderly shutdown of the server.
c. University servers must not be subjected to extremes of ambient temperature.

13.3.2 Server Configuration

a. University servers must run an appropriately licensed version of a UTPB ITS-Recognized Operating System.

b. University servers must run only necessary services. After services necessary for the essential intended purpose of the server have been identified, all other services must be disabled.

c. University servers must accept connections only to essential IP ports. After ports essential for the intended purpose of the server have been identified, all other port/socket connections must be disabled.

d. University servers must have all default account passwords changed. After determining essential default accounts, all other default accounts must be disabled.

e. University servers must have the latest systems patches applied regularly, normally within thirty days. Although promptly loading the most recent version of operating systems is not required, it is required to promptly apply all available security patches, service packs, or hot-fixes to the operating system.

f. University servers must authenticate all users to ensure only authorized users can access the resource. Supplementary authentication mechanisms should be considered for system that process or store critical or confidential information.

g. University servers must enforce password policy including requiring periodic password changes for all users (no less than once per year) and denying login after a specified number of failed login attempts. The sever must maintain a password history to prevent the reuse of recent passwords, and should be capable of testing and prohibiting the use of easily guessed (dictionary words, common acronyms, etc.) passwords.

h. University servers must have all old user accounts terminated promptly (normally within five working days.) A clear deadline must be established for account termination of persons no longer affiliated with the University.

i. University servers must have virus protection software installed and protection must be maintained at a current revision level.

j. University servers must capture and archive critical user, network, system and security event logs to enable review of system data for forensic and recovery purposes.

k. University servers may not function as a relay for SMTP or other means of relaying non-University related e-mail.

l. The server must have a limited number of user accounts with administration privileges and should have several file and access categories defined and used to prevent excess user privileges.

m. Server system and user data must be backed up in accordance with risk management decisions implemented by the Data Owner. Backup data must be encrypted in transit and at rest using industry standard encryption.

n. The server should encrypt remote administration traffic and should accept remote administration commands only from an authenticated administrator.

o. The server must use two-factor authentication for remote administration accounts, as mandated by UTS-165.

13.4 Violations

13.4.1 Any University Server determined to be noncompliant with these standards will be disconnected from the UTPB network and will remain disconnected until all compliance issues have been addressed to the satisfaction of UTPB ITS network management and the ISO.

13.4.2 Those responsible for the violation(s) may be subject to any or all of the administrative and disciplinary processes outlined in applicable operating policies and procedures of the University.

14. **Security Incident Management**

14.1 This section describes the requirements for dealing with computer security incidents. Security incidents include, but are not limited to: malware detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Electronic Mail Policy, the Internet Usage Policy, and the Acceptable Use Policy.

a. UTPB CIRT members have pre-defined roles and responsibilities which can take priority over normal duties.

b. Whenever a security incident is suspected or confirmed, the appropriate Incident Management procedures must be followed according to the UTPB Incident Response Plan.

15. **Network Access Policies**

15.1 This section establishes rules for the access and use of the UTPB network infrastructure. These rules are necessary to preserve the integrity, availability, and confidentiality of UTPB information.

15.2 Network IP addresses are provided and managed under the authority of the UTPB Information Technology Services Department. All devices connected to the UTPB network whether utilizing wired or wireless connections must conform to UTPB ITS network addressing standards. Users are permitted to use only those network addresses issued to them by ITS.

15.3 All remote access to UTPB will be approved on a case by case basis by ITS.

15.4 Users inside the UTPB firewall may not be connected to the UTPB network at the same time wireless or another connection mechanism is being used to connect to an external network.

15.5 Users must not extend or re-transmit network services in any way. The installation of routers, switches, hubs, wireless access points or other similar equipment to the UTPB network is prohibited, unless done so by ITS.

15.6 Non UTPB computer systems that require network connectivity must conform to ITS Standards.

15.7 Users must not download, install or run security programs or utilities that reveal weaknesses in the security of a system. For example, UTPB users must not run password cracking programs, packet sniffers, network mapping tools, or port scanners while connected in any manner to the UTPB network infrastructure.

15.8.1 If any weakness or security vulnerability is found by any user during the course of normal, routine access it must be reported to the CISO.

15.8 Users are not permitted to alter network hardware in any way.

16. **Encryption Practices and Sanitation Requirements**

16.1 Experience proves that many incidents involving unauthorized exposure of confidential data such as social security numbers, credit card numbers, and personal health information are the result of stolen or lost computing devices. The best way to prevent these exposures is to maintain the data in an encrypted form while at rest on the devices and maintain the physical security of these devices.

16.2 Confidential University data is not to be stored on unencrypted computing devices.

16.3 Storage of confidential University data is prohibited on personally owned computing devices.

16.4 Any confidential University data stored on a computing device must be encrypted using products and/or methods approved by the CISO.

16.5 Exceptions to section 16 may be granted only by the CISO. Requests for exceptions maybe initiated in writing by the data owner, or the CISO.

16.5.1 All exceptions must be based on an assessment of business requirements weighted against the likelihood of an exposure and the potential adverse consequences for individuals, other organizations, or the entity where an exposure could occur.

16.5.2 As a requirement for granting an exception, the CISO may require compensating controls of physical security be implemented to offset the risk created by the lack of encryption.

16.5.3 Exceptions must be documented and must include the following elements:

a. A statement defining the nature and scope of the exception in terms of the data included and/or the class of devices included
b. The rationale for granting the exception
c. An expiration date for the exception, Not to Exceed 1 year
d. A description of any compensating security measures that are to be required.
e. The CISO must approve, sign, and date all exceptions.
f. The data owner must sign and date any exception granted by the CISO.

16.6 All computer storage devices will be sanitized by ITS in a manner consistent with industry standards for that device before being sent to surplus.

17. **Computer Configuration Minimum Standards**

17.1 The ISO will recommend computer configuration updates, changes, or best practices to ITS. This section summarizes those configuration policies.

17.2 End-Users will not be configured as root or administrators on their local workstations. ITS will maintain root and administrator access.

17.3 All computers will be upgraded to the latest approved operating system for that device, or the latest operating system the device is capable of executing. If the device is unable to run the latest operating system, compensating security software will be installed.

17.4 Local files and folders will be configured in such a way to preclude access to them from other users logging into the machine.

17.5 All computers that are able to be joined to the ITS managed Active Directory Domain, will be joined to the Active Directory Domain.

17.6 All user accounts will be managed through Active Directory in accordance with Section 11.

17.7 All computers will utilize full disk encryption in accordance with Section 16.

17.8 All technology purchases will utilize ITS standards for hardware, and will require ITS and ISO approval.

17.9 All computers will have an approved version of endpoint protection software installed.

17.10 The Windows Firewall on Windows-based computers will be managed through Group Policy, and will be enabled at all times.

17.11 ITS and ISO reserve the right to dynamically change the configuration on desktop machines, as becomes necessary due to the changing technological environment or security threats.

17.12 Administrative consoles will not be installed on end-user desktop computers.

18. **Automatic Software Update Practices**

18.1 The ISO will manage security updates and patches for UTPB computers.

18.2 Windows Updates and third-party updates will be remotely installed as necessary.

18.3 Updates will normally be installed at night during non-working hours, to minimize productivity impacts on the UTPB community. However, computers that miss update cycles may have updates installed without notice.

19. **Rules of Conduct regarding Social Security Numbers (SSNs)**

19.1 The Chief Information Security Officer (CISO) at The University of Texas Permian Basin officially interprets rules of conduct and is responsible for revising them as necessary to meet the changing needs of the University.

19.2 As stated in UTS165, it is the policy of the University to protect the confidential nature of social security numbers without creating unreasonable obstacles to the conduct of business.

19.3 Employees shall comply with all provisions of UTS165 and related UT Permian Basin Administration policies and procedures.

19.4 Employees may not request disclosure of a social security number if it is not necessary and relevant to the purpose of University administration and the particular function for which the employee is responsible.

19.5 Employees may not disclose social security numbers to unauthorized persons or entities.

19.6 Employees may not seek out or use social security numbers relating to others for their own interest or advantage.

19.7 Employees responsible for the maintenance of records containing social security numbers shall observe all administrative, technical, and physical safeguards established by the university in order to protect the confidentiality of such records.

19.8 Employees shall report promptly inappropriate disclosure of social security numbers to their supervisors, who shall report the disclosure to the CISO. Reporting by the employee may be anonymous, in accordance with the University's Compliance Program, if the employee so chooses. Retaliation against an employee who in good faith reports a possibly inappropriate disclosure of social security numbers is prohibited.

19.9 Social Security Numbers will not be sent via unencrypted email.

20. **Administrative Investigations**

20.1 The purpose of this section is to establish a standard guideline for the University of Texas Permian Basin pertaining to administrative investigations based on a reasonable suspicion of inappropriate use of state information resources by a University employee. This section serves as a supplement to internal administrative policies established at UTPB and does not supersede requirements established by other university standards, procedures or policies.

20.2 The general scope of this section will apply to acquisitions of information technology hardware (e.g., computers, media, etc), software, application data, system log information and log history data as well as access to University issued machines and accounts.

20.3 This section applies to active or former, non-student, and student employees. This section does NOT apply to active or former students who have had no employment relationship with the University.

20.4 Computer forensics investigations shall not be initiated by the UTPB Information Security Office (ISO) solely for the purpose of identifying causes of poor employee work performance and/or low productivity. Employee job performance and productivity are management issues. These issues should be addressed by local management and documented through the University's established employee performance review

process. Computer forensic investigations shall be initiated only in response to suspected violations of information resource acceptable use policy.

20.5 Management will support the university's legal responsibilities and will cooperate with the Human Resources Division, the Audit/Compliance Office, the UT System Office of General Council, and UTPB ISO in the investigation and reporting of violations of University policy.

20.6 UTPB ISO will supervise all computer and network forensics investigations based on a reasonable suspicion of inappropriate use of information resources. When an investigation reveals suspected criminal activity or an investigation is initiated due to an allegation of criminal activity, UTPB IOS will work with the UTPB Police Department during all investigative activities.

20.7 When UTPB ISO investigates an administrative violation; the normal procedure for obtaining computer evidence and other information relevant to the matter under investigation shall be to impose an information requirement and/or an acquisition of evidence. UTPB ISO shall provide the requestor with a list of anticipated deliverables and due dates so to ensure all are clear about the scope of the investigation.

20.8 In certain cases involving an immediate threat to persons or property or other exigent circumstances, UTPB ISO shall take action necessary to preserve or acquire evidence and may provide evidence to law enforcement in advance of a public records request, subpoena, or warrant. In such cases the UT System Office of General Council and the UTPB Police Department shall be consulted unless circumstances make such consultation impossible.

20.9 All administrative investigations involving active or former, non-student or student employees and requiring acquisitions of information technology hardware (e.g., computers, media, etc), computer and/or network forensics, and/or access to University issued accounts must be requested in writing by the appropriate institutional Vice President. These requests shall be served directly to the University Chief Information Security Officer for handling. All such requests shall clearly allege specific information resource policy violations, based on tangible facts, warranting a forensic investigation.

20.10 UTPB ISO shall not proceed with any administrative investigations without first consulting with the UTPB Audit/Compliance Office unless exigent circumstances exist. In such cases, UTPB ISO shall consult with the UTPB Audit/Compliance Office as soon as possible.

20.11 UTPB ISO shall keep its work papers and evidence secure and limit access to only those individuals with a need to know.

20.12 The results of investigations conducted by UTPB ISO shall only be disclosed or discussed with those persons associated with UTPB who have a legitimate need to know such results in order to perform their duties and responsibilities, subject to the provisions of the Texas Public Information Act.

20.13 Information gathered and exchanged under the terms of this section shall be managed in compliance with applicable laws, rules, and regulations and shall be classified as confidential at all times.

21. **Mobile Device Configuration**

21.1 University-owned mobile devices will be enrolled in UTPB's device management software.

21.2 Bring Your Own Device (BYOD) is not permitted on the wired campus network. Wireless connectivity for BYOD is allowed provided the user has their own credentials. University information is not to be stored on unencrypted personal devices. Mobile devices can be configured to receive University email using instructions provided from ITS.

21.3 Additional requirements may be put in place for mobile devices in response to Texas law as necessary. See UTPB Prohibited Technologies Policy for more information.

22. Vendor and Third-Party Controls Compliance

22.1 Contracts of any kind, including purchase orders, memoranda of understanding (MOU), letters of agreement, or any other type of legally binding agreement that involve current or future third-party access to or creation of Information Resources and/or data must include terms determined by the Office of General Counsel as sufficient to ensure that vendors and any subcontractors or other third parties that maintain, create, or access University data as the result of the contract comply with all applicable Federal and State security and privacy laws, UTS 165, and any applicable UTPB policies or standards, and must contain terms to ensure that all University data affected by the contract is

maintained in accordance with those standards at all times, including post-termination of the contract.

22.2 The Data Owner, procurement officers and staff, IRM, and the ISO are jointly and separately responsible for ensuring that all contracts are reviewed to determine whether the contract involves third-party access to, outsourcing, maintenance, or creation of University Data; and that all such access, outsourcing, or maintenance fully complies with this Standard at all times.

22.3 Any contract involving third-party-provided credit card services must require that the Contractor provides assurances that all subcontractors who provide credit card services pursuant to the contract will comply with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) in the provision of the services.

22.4 Prior to access, maintenance, or creation of University Data by a vendor or any other third party, UTPB must ensure that an assessment is or has been performed. This assessment is designed to ensure that:

A) 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

B) 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; and

C) the vendor is TX-RAMP certified, if applicable.

22.5 As part of the assessment of a vendor or other third party, UTPB may request copies of any self-assessments or third-party assessments.

22.6 UTPB will implement access control measures as necessary to control vendor and other third-party access to its data, based on data sensitivity and risk.

22.7 Within 30 days after the termination or expiration of a purchase order, contract, or agreement for any reason, vendor must either:

A) return or securely destroy, as specified by contract or agreement, all data provided to the vendor by the institution, including all confidential data provided to vendor's employees, subcontractors, agents, or other affiliated persons or institutions; or

B) in the event that returning or securely destroying the data is infeasible, provide notification of the conditions that make return or destruction infeasible, in which case the vendor or third party must:

1. Continue to protect all data that it retains;

2. agree to limit further uses and disclosures of such data to those purposes that make the return or destruction infeasible for as long as vendor or other third-party maintains such data; and

3. To the extent possible, de-identify such data.

23. **Cloud Computing**

23.1 Confidential University data will not be stored on any cloud service, other than those officially sanctioned by ITS such as Microsoft One Drive, using the individuals UTPB credentials (Google Drive, DropBox, etc, are prohibited).

24. **Policy Exceptions**

24.1 All exceptions to this policy must be submitted via a Policy Exemption Request Form and must be approved by the requestor's supervisor, the VP of ITS, and the CISO. The Policy Exemption Request form can be found on the Information Security page in SharePoint.

Appendix A: Definitions

Authorized Agency Officer – There are two authorized agency officers at UTPB, the President and the Senior Vice President for Business Affairs

CIRT – Cyber Incident Response Team - This group is responsible for responding to security breaches, viruses and other potentially catastrophic incidents in enterprises that face significant security risks.

CISO – Chief Information Security Officer - The individual responsible for UTPB's Information Security Program.

Cloud Computing (Cloud Services) - A service that provides network access to a shared pool of configurable computing resources on demand, including networks, servers, storage, applications, or related technology services, that may be rapidly provisioned and released by the service provider with minimal effort and interaction. The term does not include telecommunications service or the act of hosting computing resources dedicated to a single purchaser.

Confidential Data - Data that is exempt from disclosure under applicable State law, including the Texas Public Information Act, and Federal laws.

Information Resources - Any and all computer printouts, online display devices, mass storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting data including, but not limited to, mainframes, servers, Network Infrastructure, personal computers, notebook computers, hand-held computers, pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and Data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

IRM – Information Resource Manager - Information Resource Managers support the professionals who protect state technology. Information technology is valuable. At state agencies, it's especially valuable because it's paid for by the people of Texas. That's why, by law, every state agency must designate an Information Resources Manager—i.e., the person responsible for overseeing IT, IT reporting, and technology compliance. UTPB's IRM is Brad Shook, V.P. of Information Technology and Analytics/CIO

Information Security Program - The policies, standards, procedures, guidelines, elements, structure, strategies, objectives, plans, metrics, reports, resources, and services adopted for the purpose of securing University Information Resources.

ITS - Information Technology Services - The Department that oversees, operates and develops policy around all things technology.

Two-factor Authentication - A process for verifying a person's identity that requires use of two of the following three elements:
(a) something the person knows, such as a password;
(b) something the person has, such as a token, authenticator app, or smart card; or
(c) a unique characteristic of the person, such as a fingerprint.