Contents

Purpose and Scope

This Procedure outlines the responsibility of end users of Texas Southmost College ("TSC") systems and network. It applies to all faculty, staff, students, student employees, trustees, contractors, business partners or volunteers who use TSC networks, systems and applications, or who access TSC Internal or Confidential data. Explicitly excluded is the general public attending events accessing any wireless network provided solely for public use. These public networks are not addressed by this Procedure. The Procedure includes guidelines on retention of documents and other information, whether in paper or electronic form.

Responsibilities

Title or Role	What They are Responsible For
Chief Information Officer	Maintains and Enforces this Procedure.
IT Professionals	Assist end users in understanding and comply with their responsibilities under this Procedure
TSC Leadership and Human Resources	Address corrective actions, as necessary, required due to non-compliance with this Procedure.
End Users	Responsible for complying with this Procedure.
Legal	Defines record retention policies for different document types, communicates exceptions (e.g. Legal holds).

Procedure

End users are responsible for protecting the information resources to which they have access. Their responsibilities cover both computerized and non-computerized information and information technology devices (paper, reports, books, film, recordings, computers, removable storage media, printers, phones, etc.) that they use or possess. Users must follow the information security practices set by the College, as well as any additional applicable information security practices required by their specific department.

Document Retention

In general, faculty and staff should retain information, including both electronic and paper documents, only as long as there is a valid business reason to keep them.

Certain business records must be kept for specific periods to satisfy federal and state law, and others should be kept for the life of the organization. Exhibit B outlines minimum requirements for record retention for different types of records. The Legal department may communicate exceptions to this Procedure in the form of Legal Holds in the event of pending litigation. Faculty and staff should ask Legal if they have questions about the retention time for specific documents.

Consent to Monitoring/ No Expectation of Privacy

End users, including faculty, staff, students, student employees, trustees, contractors, business partners and volunteers who access TSC systems and data other than the public wireless network, understand that there is no expectation of privacy, and explicitly consent to monitoring for security purposes. TSC reserves the right to routinely intercept and monitor communications for purposes including, but not limited to, penetration testing, communication security monitoring, network operations and defense, personnel misconduct, and response to potential security incidents, including capture of evidence for law enforcement purposes. At any time, TSC may inspect and seize data stored on their information

systems. Communications using, or data stored on, TSC systems are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any TSC authorized purpose. TSC systems include security measures (e.g., authentication and access controls) to protect TSC interests--not for your personal benefit or privacy.

Notwithstanding the above, using TSC systems does not constitute consent to investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services that would be considered privileged communication. This would include, but not be limited to, communication with attorneys, medical professionals, clergy, and their assistants. Such communications and work products are considered private and confidential.

Acceptable Use

TSC's intentions for publishing an Acceptable Use Procedure are not to impose restrictions that are contrary to TSC's established culture of openness, trust and integrity. TSC is committed to protecting students, faculty, staff, trustees, partners and the College from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of TSC. These systems' primary purpose are to be used for business purposes in serving the interests of the College, and of our clients and students in the course of normal operations. Limited access of the Internet for personal use is permitted, but the expectation is that:

a) The use should not interfere with the employee or contractor work responsibilities.
b) Postings by faculty, staff, students, contractors and student employees from an TSC email address to social media or newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of TSC, unless posting while performing business duties.
c) Faculty, staff, students, contractors and student employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware. If in doubt please contact the Texas Southmost College Help Desk at (956) 295- 3800 or refrain until you are able to contact the Help Desk.

Unacceptable use of TSC resources includes:

a) Engaging in any activity that is illegal under local, state, federal or international law.
b) Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products not appropriately licensed for use by TSC.
c) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which TSC or the end user does not have an active license.
d) Accessing TSC data, servers or accounts for any purpose other than conducting TSC business, even if you have authorized access.
e) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
f) Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
g) Revealing your account password to others or allowing use of your account by others. This includes fellow faculty and staff, as well as family and other household members when work is being done at home.
h) Using an TSC computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.

i) Making fraudulent offers of products, items, or services originating from any TSC account.
j) Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
k) Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
l) Port scanning or security scanning is expressly prohibited without prior notification to the CIO.
m) Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
n) Circumventing user authentication or security of any host, network or account.
o) Introducing honeypots, honeynets, or similar technology on the TSC network.
p) Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
q) Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

Effective security is a team effort involving the participation and support of every TSC faculty, staff, students, student employees, trustees, contractors, business partners or volunteers who use TSC networks, systems and applications; who deal with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly. Inappropriate use exposes TSC to risks including virus attacks, compromise of network systems and services, and legal issues. Faculty, staff, students, contractors, consultants, temporary, and other workers at TSC are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with TSC policies and standards, and local laws and regulation.

End User Responsibilities when Using E-Mail or Other Electronic Communication

As with all other College computer systems, College e-mail or other electronic communications tools are provided primarily for conducting the business of the College. College confidential information must not be shared outside of the College, without authorization, at any time. Please keep this in mind, also, as you consider forwarding non-business emails to associates, family or friends. Non-business related emails waste College time and attention.

Emails or other Electronic Communication That Discriminate

Any email content that discriminates against any protected classification including age, race, color, religion, sex, national origin, disability, or genetic information is prohibited.

Email Etiquette

The following guidelines should be observed when using College e-mail:

1. ***Only discuss public matters.*** If the matter being discussed is private, it should be discussed in private. Ask yourself if the topic being discussed is something you'd write on College letterhead or post on a bulletin board for all to see before clicking "send."
2. ***Briefly introduce yourself.*** Don't always assume the person receiving your e-mail knows who you are.
3. ***Don't "e-mail angry."*** Avoid E-mailing with bad news, firing a client or vendor, expressing anger, reprimanding someone, or disparaging other people in e-mails. These situations should be handled with face-to-face communication.
4. ***Be careful with confidential information.*** Should the e-mail get into the wrong person's hands, you could face serious, even legal, repercussions.

5. ***Refrain from sending one-liners.*** "Thanks," and "OK" do not advance the conversation in any way. Consider putting "No Reply Necessary" at the top of the e-mail when you don't anticipate a response.
6. ***Be clear in your subject line.*** Subject lines may be all someone reads, make them simple, informative, and to the point. You should proof-read your subject line as carefully as the rest of the e-mail.
7. ***Your subject line should match your message.*** Never open an old e-mail, hit Reply, and send a message that has nothing to do with the previous one. Change the subject as soon as the thread or content of the e-mail chain changes.
8. ***No more than two attachments, and provide a logical name.*** Unless it's required, don't send a message with more than two attachments. Make sure the attached files have a logical name so the recipient knows at a glance it's content and purpose.
9. ***Forward or copy others only on a need to know basis.*** Only Reply All or put names on the Cc or Bcc lines if all the recipients need the information in your message.
10. ***Pick up the phone.*** If the topic is complex or confusing, don't use e-mail. E-mail should also not be used as the only communication method for any very time sensitive communication (cancelling meetings on the same day, for instance).
11. ***Keep it short and to the point.*** The person reading your e-mail should not have to dig through several paragraphs in order to figure out what you're asking. You should state the purpose of the e-mail within the first two sentences.

End User Responsibilities when Using Personally Owned and Mobile Devices

It is understood that many end users will bring personally owned devices into TSC's facility, and potentially use them to connect to the TSC network and access TSC systems and data. While this is permitted, end users must agree in writing to follow the Rules of Behavior below prior to using their personally owned devices, by signing the Agreement to BYOD Rules of Behavior (Exhibit A).

a) Understand that participation in the BYOD program is voluntary and can be terminated by the end user at any time.
b) Unless agreed to otherwise, shall understand that participants assume all responsibility for device, accessories, and carrier service costs.
c) Shall behave in an ethical, informed, and trustworthy manner.
d) Shall abide by the law governing the use of mobile cell phones and/or smartphones; for example, while driving (*e.g.*, hands-free use and/or texting).
e) Shall follow all guidelines contained in this Procedure (IT 2.0) when accessing TSC resources.
f) Shall not attempt to override any technical or management controls and/or configurations installed as part of the BYOD program.
g) Shall immediately report loss of any device used to access TSC systems or data to the TSC. This will allow the Help Desk to remotely remove any Mobile Device Management software that may have been installed.
h) Shall notify the Help Desk prior to disposal/upgrades of BYOD device(s).
i) Shall physically protect BYOD device from theft, abuse and unauthorized use. Participants should be particularly aware of the threat of loss during periods of travel.
j) Shall use passwords to protect personally-owned equipment that meet the password complexity guidelines outlined in this document.
k) Shall protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the device.
l) Shall keep the Operating System and application software used to a current version to help protect against security vulnerabilities.

End User Responsibilities for Protecting Sensitive Data

Physical Security

Users must provide physical security for their information technology devices. Doors must be locked when possible to protect equipment when areas housing them are unattended. Special care should be exercised with portable devices which are vulnerable to loss or theft.

Information Storage

Sensitive information must be kept in a place that provides a high level of protection against unauthorized access and should not be removed from the facility. Encryption consistent with TSC standards is required for sensitive information stored electronically on all computers, and special care should be taken when electing to store sensitive information on any portable devices that are vulnerable to theft or loss. Microsoft Office or similar password protection, which also encrypts the data in the file, is acceptable, as long as the password meets minimal password complexity requirements (see below).

Distribution and Transmission of Information

Sensitive information that is transmitted electronically, transported physically, or spoken in conversation must be appropriately protected from unauthorized interception. For electronic information, appropriate encryption is required for all sensitive information, especially if that information is transmitted over public networks. Information Services Providers are responsible for employing appropriate encryption when transmitting electronic information; users must avail themselves of these services. If password protected data is sent to another individual via e-mail or other means, the associated password must be shared with the end recipient in a separate communication from the file itself.

Destruction and Disposal of Information and Devices

Sensitive information must be disposed of in such manner as to ensure it cannot be retrieved and recovered by unauthorized persons. IT should be consulted to ensure that electronic information is disposed of properly, in accordance to the guidelines outlined in InfoSec 3.0. Physical documents containing sensitive information must be shredded prior to disposal.

When donating, selling, transferring, or disposing of computers or removable media, care must be taken to ensure that sensitive data is rendered unreadable. For example, if used computers are donated or sold, all information stored on machines must be thoroughly erased. It is insufficient to “delete” the information, as it may remain on the medium. Software that rewrites random data on the medium, in accordance with InfoSec 3.0, must be used. Alternatively, the medium may be physically or electromagnetically destroyed.

Passwords

Access to computers, software applications and electronic information is frequently password controlled. Users are responsible for creating and protecting passwords that grant them access to resources. Passwords cannot be shared, displayed in plain view, or stored in computers.

Passwords used to access systems must meet password length, complexity, and longevity requirements. Although different systems may have unique password requirements, all passwords must be a minimum of 8 characters long, and must contain at least one of each of the following:

- Upper case letter (A-Z)
- Lower case letters (a-z)
- Numbers (0-9)

- Special characters (e.g. !, #, &, %, extended ASCII, etc.)

Passwords should not contain names or permutations of personal data such as social security numbers, dates of birth, etc. Default passwords must be changed on a user's first login. Generally, systems will enforce the timeframe when passwords must be changed (usually every 180 days). However, it is recommended that passwords be changed every 90 days.

Computer Security

Users must take steps to protect their desktop, laptop, and mobile devices from compromise either by the public or members of the TSC community. Users must utilize secure operating systems and software and modify default installation passwords and configurations to minimize vulnerabilities. It is the user's responsibility to either ensure or cooperate with IT to ensure that security patches are promptly installed on their laptop, desktop and/or mobile devices.

Remote Access to TSC systems

Many personal computer operating systems can be configured to allow direct access across the Internet and other networks. Users must ensure their systems are configured to prevent unauthorized access. Access to the TSC network is only authorized via the use of an approved and authorized VPN (Virtual Private Network) connection. End users can request this access via TSC.

Log Off

Users should lock their screen, or log off of applications, computers and networks when finished or when leaving the computer unattended. If computers are located in secure locations, users may not leave without locking office doors, regardless of the time they anticipate being away. Public computer users must also log off when completing their session (classroom or other shared computers. The use of boot or start-up passwords is required where unauthorized users may have physical access to non-public computers. Users should not disable their auto-off monitor function, which requires a password to reactivate their session.

Virus and Malicious Code Protection

Users must ensure that their personal computers employ mechanisms that protect against viruses and other forms of malicious code which may be distributed through email or the web. Users must have anti-virus software loaded on any device used to access the TSC network from off-site. To ensure that virus protection remains effective, individuals must install new versions as they become available.

Because no anti-virus software is effective against all viruses, users must exercise caution when opening email or downloading files from the Internet. Users should not open unexpected or suspicious attachments and should configure word processing, spreadsheet, and other applications to require user confirmation before macros, scripts, or other executable enclosures are opened. Confirmation should be granted only if the source of the file is known or trusted.

If a virus is detected, it must be immediately and completely eradicated before email or files of any sort are sent to other users. After contamination is eliminated, individuals who may have been sent infected files must be informed by telephone or other non-electronic means. All potentially infected files, including those stored on network servers and backup media must also be examined for infestation and treated accordingly.

Detecting and Reporting Potential Security Incidents

Users must report suspected compromises of information resources, including contamination by computer viruses, to their managers and TSC (who will inform the Incident Response Team, who in turn will proceed in accordance with IT 3.6, IT Security Incident Response). Incidents must be reported on the same business day users become aware of the potential compromise. Below are a few signs your accounts or systems may have been compromised. These are only examples – the threat landscape is constantly changing, and you should report ANY behavior that appears out of the ordinary.

- Fake antivirus messages – a warning about a potential virus that requires you to click on a link or button. Typically, taking the indicated action actually installs the Malware on your system.
- Unwanted browser toolbars – These are often installed as a result of downloading unsafe software or visiting unsafe Internet sites.
- Redirected Internet searches – if you search for common terms but end up somewhere unrelated, it may be a sign that there is Malware redirecting your activities.
- Frequent random popups – If you see popups from websites or when using programs that don't usually generate them, it may indicate Malware on your system.
- Fake e-mails from your account – If your colleagues or friends start receiving e-mails that are from your account, it's a good indication you've been compromised.
- Your online passwords suddenly change – this could be an indicator that either your system OR the online service (or your specific account) are compromised.
- Unwanted or unexpected software installs – if you see software installed unexpectedly, it's a pretty sure sign your system has been compromised.
- Your mouse moves by itself and makes selections – This is a very sure sign of compromise.
- Your antivirus, task manager, or registry editor is disabled and can't be restarted. Malicious programs do this to protect themselves.
- Your bank account shows unexpected transactions – this could be result of your system being compromised and interception of your account information.
- You get calls from stores about nonpayment of shipped goods – this may be a sign that one or more of your accounts has been compromised.
- You suddenly can't access files on your system – this is often accompanied with some form of message requesting payment to restore access. This is typically called "Ransomware".
- You are asked for your username or password.

Again, this is not a complete list, and ultimately, you should err on the side of caution and report any activity that appears unusual or suspicious.

Consequences of Not Complying with this Procedure

The greatest consequence of end user non-compliance of this Procedure is that it will put TSC systems and data at risk. End users may be subject to disciplinary action, up to and including termination of employment. In addition, students may be subject to disciplinary action (refer to student handbook). Unlawful activity may also be subject to civil and criminal penalties, as required by law. Any disciplinary action resulting from violation of this Procedure will be coordinated with Human Resources (HR) to ensure compliance with HR policies and relevant employment law.

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this Procedure.

1. IT 3.0, IT Security for IT Professionals

2. IT 3.6, IT Security Incident Response

Exhibits

This section contains links to any documents that are required to be used by the Procedure.

Exhibit A	Acceptance of IT 2.0 End User Responsibilities and Bring Your Own Device (BYOD) Rules of Behavior
Exhibit B	Document Retention Schedule

Exhibit A – Acceptance of End User Responsibilities and Bring Your Own Device (BYOD) Rules of Behavior

End users must review and indicate their understanding, acceptance, and agreement to abide by IT 2.0, End User Responsibilities and the Rules of Behavior below, prior to accessing TSC's network, systems or data.

A. I agree that I understand and will abide by the End User Responsibilities outlined in IT 2.0.

B. I understand that participation in the BYOD program is voluntary and can be terminated by the end user at any time.

C. Unless agreed to otherwise, I understand that participants assume all responsibility for device, accessories, and carrier service costs.

D. I shall behave in an ethical, informed, and trustworthy manner.

E. I shall abide by the law governing the use of mobile cell phones and/or smartphones; for example, while driving (*e.g.*, hands-free use and/or texting), especially when conducting College business.

F. I shall follow all guidelines contained in this Procedure (IT 2.0) when accessing TSC resources.

G. I shall not attempt to override any technical or management controls and/or configurations installed by TSC, either on TSC devices or on personal devices used to access TSC systems or data.

H. I shall immediately report loss of any device used to access TSC systems or data to the TSC. This will allow the Help Desk to respond to the risk of data loss or systems compromise.

I. I shall notify the Help Desk prior to disposal/upgrades of BYOD device(s), so that they can confirm if necessary there is no College data or access to College systems (e.g. e-mail) left on the device prior to disposal/upgrade.

J. I shall physically protect BYOD device from theft, abuse and unauthorized use. Participants should be particularly aware of the threat of loss during periods of travel.

K. I shall use passwords to protect personally owned equipment that meet the password complexity guidelines outlined in this document.

L. I shall protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the device.

M. I understand that TSC may need to remotely wipe TSC data off of devices, including any personal devices I use to access TSC systems or data, in the event of loss of a device or my termination. I also recognize that while TSC data will use reasonable attempts to limit this data wipe to TSC data, that it is possible that non-TSC data may also be lost in the process.

Name: _____

Signature: _____

Date: _____

Exhibit B – Document Retention Schedule

Type of Information	Retention Guideline	Notes
Business Records		
• Articles of Incorporation • Bylaws • Annual financial filings • Board policies and meeting minutes • Board and Board Committee minutes • Construction documents • Fixed asset records • Audit reports, from independent audits • Corporate resolutions • Determination Letter from the IRS, and correspondence relating to it • IRS Form 1023 (Application to file for charitable and/or tax-exempt status) • Sales tax exemption documents • Financial statements (year-end) • Real estate deeds, mortgages, bills of sale • Tax returns	Permanent	
• Contracts	Permanent if current (7 years if expired)	
• Marketing, Advertising, Promotional and Sales Materials	3 years; except invoices, contracts, leases, licenses and other legal documents should be retained for 3 years beyond the life of the document	
• Sales and purchase records	3 years	
• Donor records and acknowledgement letters	7 years	
HR Records		
Employee records	Kept for 7 years after termination, unless otherwise required by law	Employee records may or may not be maintained by the HR department
• EEO-1 Reports (Employer Information Report)	Filed annually, most recent kept on file	
• Pension plan and retirement records	Permanent	
• Employee benefit plans subject to ERISA (includes plans regarding health and dental insurances, 401K, long-term disability and Form 5500)	6 years from when the record was required to be disclosed	
• Workers' compensation records	Duration of employment + 30 years	
Health, Medical and Safety data		

• Injury and Illness Incident Reports (OSHA Form 301) and related Annual Summaries (OSHA Form 300A); Logs of work-related injuries and illnesses (OSHA Form 300)	7 years following the end of the calendar year that these records cover	Keep health, medical and safety data separate from other employee records
• Hazardous material exposures	Duration of employment + 30 years	See above
• Requests for accommodation and disability	1 year	See above
• Medical exams required by law	Duration of employment + 30 years	See above
• Toxic substance exposure records	30 years	See above
• Blood-borne pathogen exposure records	30 years	See above
• Family Medical Leave Act (FMLA)	3 years	See above
Accounting, Finance and Tax Records		
• Accounts Payable and Receivable ledgers and schedules • Bank statements; cancelled checks and deposit slips • Business expense records • Electronic fund transfer documents • Employee expense reports • Invoices • Filing of fees paid to professionals (IRS Form 1099) • Payroll tax withholdings • Earnings records • Payroll tax returns	7 years	
• Annual audit reports and financial statements • Cash receipts • Check registers • General ledgers • Journal entries • State unemployment tax records	Permanent	
• Annual plans and budgets	2 years	
• Depreciation, Asset Retirement Records	4 years	
• Petty cash vouchers	3 years	
• Annual tax filing for the organization (IRS Form 990 in the US)	Permanent	
Legal and Insurance Records		
• Appraisals • Copyright restrictions • Development/Intellectual Property/Trade Secrets • Due diligence files • Environmental studies • Insurance claims/applications • Insurance disbursements and denials	Permanent	

• Insurance policies (Directors and Officers, General Liability, Property, Workers' Compensation) • Litigation files (excluding liability claims) • Patents, patent applications, supporting documents • Real estate documents (including loan and mortgage contracts, deeds) • Stock and bond records • Trademark registrations, evidence of use documents		
• Leases	6 years after expiration	
• Memoranda of Understanding; Letters of Intent	5 years beyond the expiration date	
• Press releases	4 years	
• Warranties	Duration of warranty + 7 years	