Information-Security Responsibilities of All Users of TAMUCC Information Resources

All users TAMUCC information resources must use those information resources in a responsible manner. The primary TAMUCC policies in this area are Procedure 29.01.99.C1.01 "IT Acceptable Use and Privacy (ITAUP)" and the "IT Standards for All Users (ITSOC)." Below is a brief summary of the most important responsibilities as outlined in those documents. However, the ITAUP and the ITSOC are the official documents with regards to TAMUCC. These responsibilities are the baseline responsibilities of all users. A user may have additional responsibilities if they are the Owner or Custodian of an information resource.

- Keep **personal use of University information resources** (e.g., your University desktop workstation) to a minimum.
- **Protect your privacy.** Anything you store on a University information resource (e.g., your files and emails) and anything you send or receive via the University network is logged by the University and may be examined by authorized University personnel.
- **Protect your University passwords.**
  A. Do not disclose your University passwords to anyone else for any reason.
  B. Do not fall prey to "phish" emails that ask you to disclose your username and password.
  C. Log in to the University network with only your password. Do not log in to the network with anyone else's password.
  D. If anyone else discloses their network password to you, or you learn that someone else has disclosed their password to others, it is your duty to notify the Office of Information Security.
  E. If you believe that your password has been compromised (i.e., someone else now knows it), you must 1) change the password immediately and 2) notify the Office of Information Security
- **Protect the University's confidential/sensitive information.**
  - Definitions
    - Confidential information includes student grade information, health care information, social security numbers, and credit card/bank account numbers.
    - Sensitive information includes University operational documents, personnel records, research data, and internal communications.
    - These are just examples - contact ois@tamucc.edu if you are in doubt.
  - Only the Owner of the confidential/sensitive information may determine who can access that information and how it can be shared or otherwise used. Make sure you know the Owner's rules regarding the handling of the Owner's confidential/sensitive information. Users must not use such data for personal purposes without the express prior approval of the Owner.

    - Confidential/sensitive information should not be stored on a portable device unless absolutely necessary, and should be deleted from that device as soon as possible.
    - Per Texas state law, confidential/sensitive information in your possession must be encrypted if it is:
        - Stored on any portable device (e.g., USB stick, smartphone, laptop), OR
        - Stored on any non-University computer (e.g., your home computer), OR
        - Sent via email outside of TAMUCC (e.g. via the Internet).
- **Protect your workstation**: log off, shut down, or lock the desktop when you walk away from your workstation.
- **Receive the mandatory information security training.**
    - Upon first receiving their network username and password, and every two years thereafter, each user must take and pass the Information Security training course on TrainTraq.

Protecting Your Passwords

What does 'unauthorized disclosure' of my password mean?

Your passwords to University computer systems are property of the University. The University has entrusted you with these confidential passwords, and only the University can authorize the disclosure of these passwords to anyone else. University policy is that your password is to be disclosed to nobody else, period. A user who discloses their password to another user can be subject to discipline, as can a user who logs in with another user's username and password.

How does unauthorized disclosure of passwords typically happen at the University?

Most password disclosures are due to phishing. In phishing, a user is deceived into disclosing their own password to someone else. Phishing is a serious threat and is discussed at length in our phishing page. Other typical scenarios include supervisors asking subordinates for their passwords, or supervisors sharing their passwords with subordinates so that the subordinate can approve documents on the supervisor's behalf or read the supervisor's emails. Understand that these practices not only violate University information-security policy but also violate System policy regarding fraud and separation of duties.

Why is disclosing a password such a big deal?

When User A discloses their password to Person B, Person B can now log in as User A and view any confidential information to which User A had access. This results in several problems. First, Person B may be malicious and misuse the confidential data to perform identity theft, which harms the people (i.e., the 'owners') identified in the confidential information. Second, if the owners of the confidential data are harmed by the unauthorized disclosure, the University may be subject to fines and lawsuits. Third, even if confidential information is not misused, the University typically is legally obligated to notify the owners and various government agencies of any such unauthorized disclosure, which is time-consuming and damages the University's reputation.

How do I protect my passwords from unauthorized disclosure?

- **Do not give your computer passwords to anybody, ever.** Make some time and read our phishing page. The core message is to never give your passwords to anyone, ever. Following this one simple rule is the single most important thing you can do for the University's information security.

- If you need to store your passwords, then use a *password safe*, a specialized program for securely storing passwords. There are many free password safe programs available on the Internet. Perhaps the most popular is KeePass, a free program that works on PCs, Macs, Linux, and smartphones. You store all your passwords in the password safe then lock the safe with a very strong password or passphrase. Now all you have to remember is that password/passphrase. You can then store the safe on a cloud service like Google Drive or Dropbox. Now you can access your passwords from any Internet-connected computer.

- Do not write your passwords on a post-it note and stick it to the bottom of your keyboard. Do not write your passwords into a Word document and store it on your hard drive without encrypting it. These practices are forbidden by University policy.

Protecting Confidential Information

The most important information-security responsibility placed on all users of TAMUCC's computer systems is the duty to protect the confidential information in the University's possession.

Unauthorized disclosure of confidential information can result in identity theft and other harm for those people whose confidential information was disclosed.

Unauthorized disclosure of confidential information can result in fines, litigation, and embarrassment for the University.

Users who do not protect confidential information can be subjected to discipline.

What is Confidential Information?

The simple answer is that confidential information breaks down into two main types:

1. Information about other people including:

- Personally Identifying Information ("PII") such as social security numbers and Banner IDs;
- Student Educational Records, such as course and grade information;
- Credit Card Numbers and other financial account numbers;
- Personal Health Information ("PHI")

2. Your password(s). Your passwords are confidential information that belongs to the University, and your passwords help protect other confidential information.

How Do I Protect Confidential Information?

How do I protect the confidential information in the University's possession?

Protect Your Passwords

Passwords are the primary mechanism for protecting confidential information. Choose strong passwords and **do not disclose your passwords to anyone else, period.**

Avoid Local Copies

Most confidential information at the University is stored in secure databases such as Blackboard, Banner, and FAMIS. That's where it belongs. Most incidents regarding confidential information involve *local copies*, i.e., chunks of confidential information that are stored outside these secure databases. A classic example is the gradebook which is stored as a spreadsheet on a laptop. The best way to avoid problems with local copies is to not create them at all. Use Blackboard instead of an individual gradebook file.

Use Encryption

If you must use a local copy, make sure either 1) the local copy itself is encrypted or 2) the local copy is stored on an encrypted device. Texas state law requires confidential information to be encrypted when it is either 1) stored on any portable device, 2) stored on any non-state-owned computer (e.g., your home computer, Dropbox), or 3) transmitted over the Internet.

Protecting Electronic Grade Information

1. Summary

This document explains the rules regarding the secure storage and transmission of electronic student grade information, and how University users can comply with those rules.

Electronic grade information is confidential information per federal and state law (see "Discussion of the Rule" below). Therefore, users in possession of electronic student grade information must encrypt that information when it is:

1. stored on either a) any portable device (laptop, tablet, phone, or flash drive) or b) any non-state owned computer (e.g., home computer, Google, Dropbox), or;
2. transmitted over the Internet.

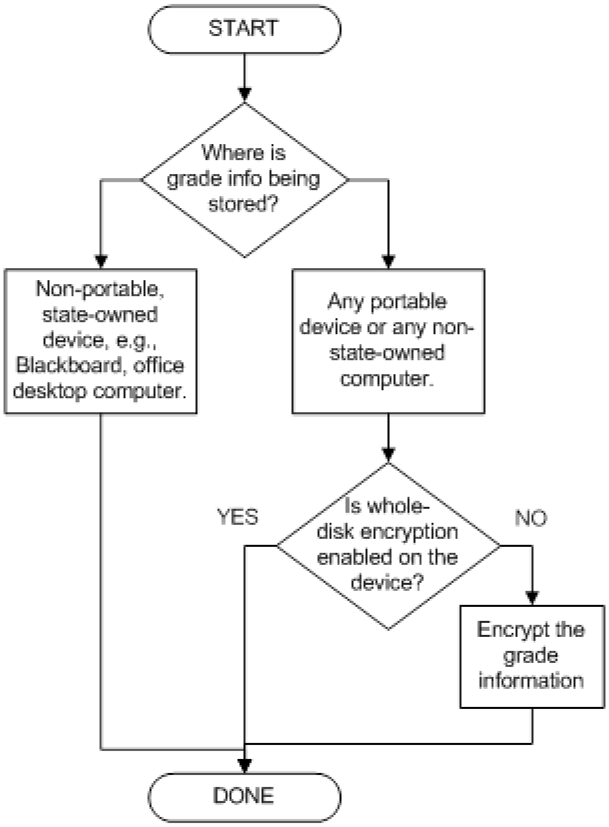
Acceptable methods for transmitting electronic grade information:

- Blackboard
    - Have students log into Blackboard to retrieve their grades.
    - Use Blackboard's "messaging" feature (not Blackboard's email feature).
- via Internet Email ONLY IF:
    - You use secret codes for students instead of their real names and send all grades to all students in class OR
    - You encrypt the file containing the grade information.

Acceptable methods/locations for storing electronic grade information:

- In Blackboard;
- On a University-owned desktop computer;
- On a portable or non-state owned computer ONLY IF:
    - The device has whole-disk encryption enabled and/or;
    - The file containing the grade information is encrypted.

Here is a flowchart showing the decision tree for storing electronic grade information.


START
Where is grade info being stored?
Non-portable, state-owned device, e.g., Blackboard, office desktop computer.
Any portable device or any non-state-owned computer.
YES
Is whole-disk encryption enabled on the device?
NO
Encrypt the grade information
DONE

2. Discussion of the Rule

Texas state law TAC 202.1(3) defines confidential information as "*[i]nformation that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act, and other constitutional, statutory, judicial, and legal agreement requirements).*"

FERPA is a federal law that protects student grade information from unauthorized disclosure and public release. Ergo, student grade information is confidential under Texas state law.

Texas state law TAC 202.75(4)(A) states that *"[c]onfidential information that is transmitted over a public network (e.g.: the Internet) must be encrypted."* Texas state law TAC 202.75(4)(C) states that *"confidential information must be encrypted if copied to, or stored on, a portable computing device, removable media, or a non-agency owned computing device."*

3. Frequently Asked Questions

Q: **What is whole-disk encryption?** A: For storage on a portable or non-state-owned computer, an alternative to encrypting individual files is to encrypt an entire hard drive aka “whole disk encryption.” With whole disk encryption, any file stored on that disk is automatically encrypted. Windows comes with a free whole disk encryption program called BitLocker; OS X comes with a program called FileVault. Most University-owned Windows laptops already have BitLocker turned on, so you can safely store grade information on these laptops without encrypting individual files. If you are unsure whether your University-owned laptop has Bitlocker turned on, please call the IT Department at x2692.

Q: **How do I encrypt individual electronic files?** A: Many common programs, such as Microsoft Word and Excel, offer the ability to encrypt the documents and spreadsheets you create in them. For example, in Microsoft Excel, you choose Home > Prepare > Encrypt. Also, there are free encryption programs that you can download from the Internet. You can use these programs to encrypt/decrypt any kind of file. The IT Department has been evaluating several of these programs and currently recommends MEO from NCH software. This program is simple, free, and works with both Windows and OS X systems. The only downside of MEO on Windows systems is that the program installs various placeholders for other free NCH programs, which can show up on your Start menu and genuinely make a nuisance of themselves, but they are easy to delete.

Q: **Can I transmit unencrypted grade information to a student’s Islander account?** A: Yes, but be careful. It must be sent to the student’s Islander email account, not their personal account. And make sure you only send student A’s information to student A. Frequently, faculty make mistakes and end up sending other students’ information, which is FERPA event that must be documented and filed with the Department of Education. Blackboard/Banner is the more secure way of communicating grades to students.

Q: **Can I transmit unencrypted grade information via Blackboard?** A: Yes, but you have to be careful. Blackboard offers two ways to transmit information to people: email and "messaging." Email is a traditional email service that actually sends the entire message to the recipient. In contrast, messaging stores your message on the Blackboard servers and transmits only a notification to the recipient saying that a message is waiting for the recipient on Blackboard. The recipient then needs to log into Blackboard to get their message. Unencrypted grade information can be communicated via the messaging function, whereas such information cannot be sent via Blackboard's email function.

Q: **Can I store my unencrypted grade information on cloud storage services like Google Docs and Dropbox?** A: No. Because cloud storage services are non-state-owned computers, you may grade information on cloud services only if it is encrypted. None of the major cloud services encrypt, so it's up to you to encrypt. So if you keep your gradebook in an Excel spreadsheet that you want to copy it to your USB thumb drive (a portable device) or to Google docs (a cloud service), then you must encrypt it.

Q: **Can I stored my encrypted grade information on cloud storage services like Google Docs and Dropbox.** A: Yes. Watch out, however, if you are using the web to create the document, not just store it. For example, Google has a full suite of online programs for creating word processing documents and spreadsheets. There is no way to encrypt these documents online.

Q: **Can I transmit my unencrypted grade information using secret codes instead of student names?** A: Yes, as long as 1) the secret code is truly random, 2) the code for a given student is known only to the given student and yourself, 3) all grades are sent to all students, and 4) the listing of all grades is itself totally random, i.e., not sorted on some public information like last name.

Q: **Can I request that that students use their Islander email account when corresponding with me?** A: You can certainly ask, and you can make a policy that you will not answer student-related questions in email unless it is from the student's Islander email address. However, there is nothing that IT can do with technology to force students to communicate with you only by Islander.

Q: **When I send an email to "All Student Users" in Blackboard, does this go to their Islander email, or can it go to another email address?** A: It can go to another address. The default is the student's Islander address, but students can go in and change that value.

Q: D**o I have to protect all grade information, or just the final grade in a class?** A: All grade information.

4. For Further Information

Please contact the Office of Information Security: ois@tamucc.edu.

OIS: FAQs: Encryption

What is Encryption?
Encryption is the process of taking a file (the *cleartext*) and scrambling (*encrypting*) that cleartext file to generate a second, scrambled file (the *ciphertext* or encrypted file). The scrambling is performed by a computer program known as an *encryption algorithm*. You tell the encryption algorithm how to encrypt the cleartext by supplying a secret password also known as an *encryption key*. The ciphertext looks like gibberish and cannot be *decrypted*, i.e., turned back into the cleartext, unless you have the key.

Why would I want to encrypt a file?
Typically, because the file contains confidential information. Every University user has a central duty to protect confidential information. That includes not only your own computer passwords, but also the financial, academic, and medical records of others entrusted to the University. Typically, that confidential information of others is kept in secure, central databases, but there may be times when some of that information needs to exported to another file (a *local copy*) so that it can be shared with another party, or worked on at home by an employee.

Local copies are troublesome because they are apt to be forgotten and misplaced. As such, they can be discovered by others, resulting in the unauthorized disclosure of confidential information. If, however, the local copy is an encrypted file, it will be unreadable to anyone who does not have the key.

What are the typical situations where I would encrypt a document?
Any time you have a file that contains confidential information. Typical examples:

- A Word document that contains all of your usernames and passwords for various accounts;
- A spreadsheet containing the names and grades of students taking your class;
- A spreadsheet containing the social security numbers of everyone in your department;
- PDF medical records of all the people in your test group.

How do I encrypt a document?
By using an encryption program. There are several programs for free on the Internet. The Information Security Office has used several of these: MEO, AxCrypt and TrueCrypt.

Avoiding Identity Theft

The following tips can help lower your risk of becoming a victim of identity theft.

- **Protect your Social Security number.** Don't carry your Social Security card or other cards that show your SSN. Read, "Identity Theft and Your Social Security Number."
- **Use caution when giving out your personal information.** Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in emails and in postal mail.
- **Treat your trash carefully.** Shred or destroy papers containing your personal information including credit card offers and "convenience checks" that you don't use.
- **Protect your postal mail.** Retrieve mail promptly. Discontinue delivery while out of town.
- **Check your bills and bank statements.** Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It might mean that someone has changed contact information to hide fraudulent charges.
- **Check your credit reports.** Review your credit report at least once a year. Check for changed addresses and fraudulent charges.
- **Stop pre-approved credit offers.** Pre-approved credit card offers are a target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. **Call toll-free 888-5OPTOUT (888-567-8688)**.
- **Ask questions.** Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. If you're not satisfied with the answers, don't give your personal information.

- **Protect your computer.** Protect personal information on your computer by following good security practices.
- Use strong, non-easily guessed passwords.
- Use firewall, anti-virus and anti-spyware software that you update regularly.
- Download software only from sites you know and trust and only after reading all the terms and conditions.
- Don't click on links in pop-up windows or in spam email.
- **Use caution on the web.** When shopping online, check out a website before entering your credit card number or other personal information. Read the privacy policy and take opportunities to opt out of information sharing. Only enter personal information on secure web pages that encrypt your data in transit. You can often tell if a page is secure if **"https"** is in URL or if there is a padlock icon on the browser window.

Steps to Take if Your Data Becomes Compromised or Stolen

If you have reason to believe your personal information has been compromised or stolen, contact the Fraud Department of one of the three major credit bureaus listed below.

A recent amendment to the Federal Fair Credit Reporting Act requires each of the nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months. Be aware that there's only one online source authorized to do so, annualcreditreport.com. For more information, please visit the Federal Trade Commission's page on obtaining your credit report at no cost. However, if you still need to contact the credit reporting agencies directly, contact by telephone or mail may be the most reliable method. **Be cautious if requested to provide personal information over the Internet unless you are absolutely sure of the validity of the site.**

Equifax
www.equifax.com
1-800-525-6285

Experian
www.experian.com
1-888-397-3742

TransUnion
www.transunion.com
1-800-680-7289

Policy

There are various laws and policies that govern information security at TAMUCC.

1. General Information Security Laws and Policies

TAMUCC Rules and Procedures

The University's Rules and Procedure regarding information resources are found in Section 29. These policies apply to only TAMUCC.

A&M System Policy and Regulations

Section 29 contains policy regarding information resources. These policies govern all A&M institutions.

Texas Administrative Code, Chapter 202 ("TAC 202")

This is the key Texas state law regarding information security. Much of System and TAMUCC policy is derived from TAC 202.

Summary of Information Security Responsibilities of All Users

Not itself a policy, but a summarization of key provisions of TAC 202, System, and TAMUCC policy that apply to all users of TAMUCC information resources.

2. Specialized Information Security Laws and Policies

Higher Education Opportunity Act ("HEOA")

Family Educational Rights and Privacy Act ("FERPA")

FERPA is a federal law governing the handling of certain types of student information, especially grades.

Red Flags Rule "RFR"

The Red Flags Rule is a federal standard that aims to prevent identity theft.

Payment Council Industry ("PCI")

PCI is a set of standards put forth by the credit card industry. TAMUCC business units that conduct credit-card transactions must comply with the PCI Data Security Standard, or PCI-DSS.

Support Information

Please contact the Information Technology Help Desk at x2692 for additional assistance.