Secure Our Systems

University of Houston System

UNIVERSITY of HOUSTON

UNIVERSITY of HOUSTON

Secure Our Systems (SOS) Training

The purpose of Information Security Awareness Training is to educate employees on how to protect confidential and sensitive information maintained by the University of Houston System and its universities.

The Texas Government Code, Texas Administrative Code Information Security Standards (TAC 202) and the Gramm-Leach Bliley Act (GLB Act), as well as other regulations and state and federal laws, require training for all System employees.

Topics Covered

1. Information Security
2. Data Classification & Protection
3. Information Security Incidents
4. Best Practices to Safeguard Information & Information Systems
5. Email Security
6. Identity Theft
7. Copyrighted Material
8. Gramm-Leach-Bliley Act (GLB Act)
9. Health Insurance Portability and Accountability Act (HIPAA) and Texas Medical Record Privacy Laws

Information Security

Information Security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

Information security risks arise from the loss of confidentiality, integrity, or availability of information or information systems and may potentially have an adverse impact to the University of Houston System and its universities.

Information Security

The University of Houston System and its universities are vulnerable to attacks from hackers, phishers, spammers and other intruders known as threat actors.

These attacks are an attempt to gain unauthorized access to services, resources or information in an attempt to compromise the integrity, availability of confidentiality of university data.

The threat to the University of Houston System and its universities is to cause an adverse impact to the mission, daily operation, image or reputation of the System and its universities by destroying or modifying information, and/or attempting a denial of service attack.

Data Classification & Protection

The University of Houston System classifies data in three ways:

Level 1

Confidential Information

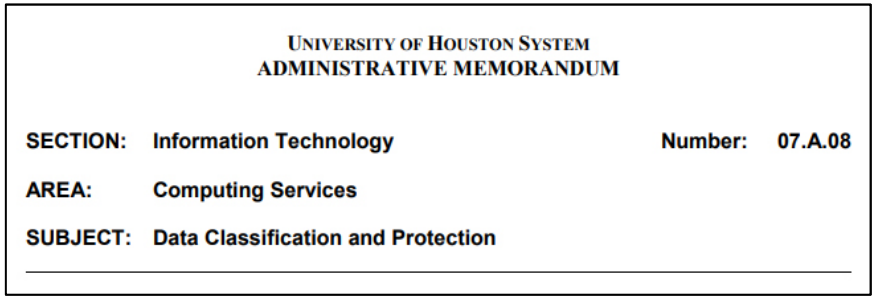
- Social security number
- Educational records (FERPA)
- Healthcare information (HIPAA)
- Customer information (GLB)

Sensitive Information

- Individual's name in combination with social security number, government-issued identification number (i.e., driver's license number), or account number with required security code or password
- Individually identifiable information related to an individual's health care

Mission-Critical Information

- Information defined by the university or information owner to be essential to the continued performance of the mission of the university.



UNIVERSITY OF HOUSTON SYSTEM
ADMINISTRATIVE MEMORANDUM

SECTION: Information Technology Number: 07.A.08

AREA: Computing Services

SUBJECT: Data Classification and Protection

Level 2

Protected Information

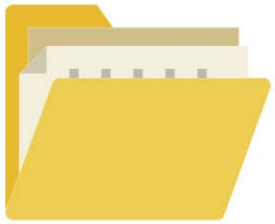
- Information that may be subject to disclosure or release under the Texas Public Information Act as requested.

Level 3

Public Information

- Information readily available in the public domain, such as information posted on the component university's public web site, and any other information not classified as Level 1 or 2.

Data Classification & Protection



Employees are responsible for protecting Level 1 data in any form, electronic or paper, no matter the location.

Per University of Houston System policy, SAM 07.A.08, Level 1 data must be stored in an appropriately protected location, such as university provided file storage or university systems such as PeopleSoft and Blackboard.

A significant number of university data breaches occur when Level 1 data is lost or stolen from a laptop, removable media device (e.g. portable drive, CD/DVD, media card). Any device containing Level 1 should be disposed of or sanitized in accordance with SAM 07.A.08.

What is an Information Security Incident?

Information security incidents involve an actual or imminent breach of information security as it relates to information maintained by the University of Houston System and its universities.

Specifically, an information security incident may include:

- Unauthorized access of university data
- Unauthorized use of a user's account
- Unauthorized copying or distribution of copyrighted or licensed software or data
- Misuse of computer resources

Reporting an Information Security Incident

When an employee believes an information security incident has occurred, the UHS Information Security team should immediately be notified in one of the following ways:

Email

- UH - security@uh.edu
- UH-Clear Lake – security@uhcl.edu
- UH-Downtown – security@uhd.edu
- UH-Victoria – security@uhv.edu

Call:

- UH – (832) 842-4695
- UH-Clear Lake –
- UH-Downtown –
- UH-Victoria – (361) 485-4505

To report an incident anonymously, visit the UHS Fraud & Non-Compliance Hotline. A link to the Hotline is located at www.uh.edu.

Stolen Equipment?

To report theft of your personal device on campus or theft of a university owned device, file a police report with the appropriate campus police department IMMEDIATELY!

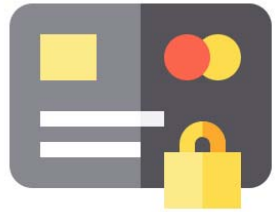
- UH Police – 713-743-3333
- UH-Clear Lake Police – 281-283-2222
- UH-Downtown Police – 713-221-8065
- UH-Victoria Police – 361-570-HELP (4357)
- UHS Sugarland Police – 281-275-3302

Best Practices to Safeguard Information & Information Systems

- Ensure that computers are up-to-date with security software updates/patches
- Ensure the latest anti-virus software is installed
- Ensure operating system and all application software are up-to-date
- Log off or lock computers when away from work area
- Place computers on standby or sleep mode at night and during holiday breaks to minimize hacking activities

Best Practices to Safeguard Information & Information Systems

- Backup files on a regular basis
- Eliminate storage of Level 1 data (i.e. Social Security numbers, etc.) where possible
- Comply with federal, state, UHS and university requirements for information security
- Use a strong password and follow good password management practices



Credit card information should ***never*** *be stored on individual computers*

Password Management

Minimum Password Length: 8 characters

Consider using a pass phrase

Passwords must contain at least one character from each of the following groups:

- Alphabetic: Upper or lower case (a-z, A-Z)
- Numeric: 0-9
- Special Characters: ! $ % & ( ) * @ ^

Change your password at least every 180 days

Do not share your passwords with anyone…ever

Use a unique password for different types of accounts (work, personal email, personal banking, etc.)

Email Security

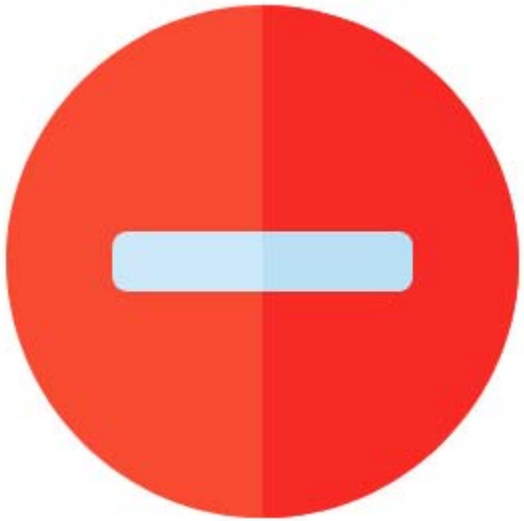
Email is not private and can be intercepted, altered, or used to carry out crimes, including collecting your personal information.

Avoid becoming a victim – protect yourself against malware, viruses and information theft.

An email virus is a program or piece of code that is sent to computer users as an email attachment. The virus is activated when the attachment is opened.

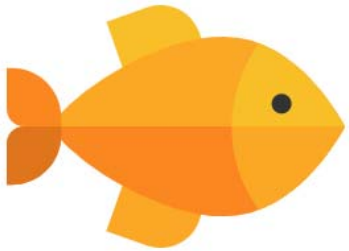
Take Action: Email Security Tips

Delete, **do not open**, email messages with attachments you are not expecting. The attachment may contain malware or a virus.



Do not reply to spam or click the “Remove From Mailing” link in a spam message. Doing so will let spammers know they have reached an active email account and the amount of spam you receive will only increase.

Phishing Email



Phishing is not similar to the fun and relaxing outdoor pastime that comes to mind. Phishing is so named because computer spammers use fraudulent email messages to “fish” for personal financial information.

For example, phishing emails may ask you to provide personal information in order to verify or reinstate your banking privileges.

- Phishing emails are designed to be difficult for recipients to recognize.
- Phishers know they must gain your trust before you respond.

Listed on the next few slides are some common tricks phishers employ to make emails and website look and act legitimate.

Phishing Email

Phishing messages:

- Mimic reputable companies and can often include links to fake sites that appear to be real
- Appear to originate from a reputable company, but are often set to reply to a fraudulent address
- Appear to be official looking messages
- Usually don't allow much time to collect information. Their messages often claim the recipient has 24 hours to respond
- Assures the recipient that the transaction is secure and private and often will include TRUSTe symbol in order to appear legitimate

Taking Action: Email Phishing Tips

- **Do not reply** to email messages asking for your personal information
- **Do not click** links in email messages. Instead, type the address directly into the browser address bar
- Look for official contact information in an email message requesting you take action
- Remember that companies **will not ask** you to verify your user name and password via email
- View the site's certificate to verify the company

Identity Theft

What is it?

Identity theft occurs when someone without your knowledge or permission uses your name, social security number, date of birth, bank or credit card account number or other identifying information to commit fraud or other crimes.

When does it occur?

Identity theft occurs when someone gains unauthorized physical access or network access to computers to steal university information. Phishing is one of the most common methods that thieves use to obtain personal information.

Identity Theft

Here are some signs that may indicate you have already become a victim of identity theft:

Bills do not arrive as expected

Denials of credit occur for no apparent reason

Unexpected credit cards or account statements are opened in your name

You receive calls or letters about purchases that you did not make

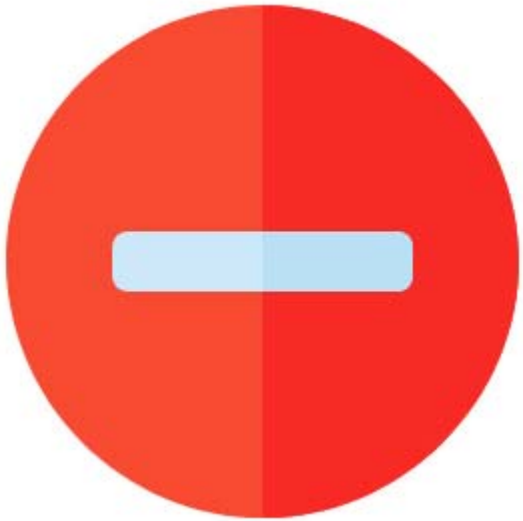
Take Action: Identity Theft Tips

Here's what you can do to avoid becoming a victim of identity theft:

- Shred financial documents
- Don't use obvious passwords like your birth date, address, phone number, pet names, etc.
- Avoid spoofed sites by typing the URL directly into your browser's address bar
- Close any accounts that have been tampered with or established fraudulently
- Monitor your credit report regularly

Downloading Copyrighted Material

Downloading copyrighted material from Internet sites such as documents, images, movies, games and other types of software without approval from the author or organization that owns it is a violation of copyright laws.



Avoid sites that allow you to download or upload copyrighted material for “free.” If you do so, you are subject to legal prosecution for copyright infringement.

Using Copyrighted Material

An important limitation to copyright law is the concept of fair use. Fair use allows for the limited use of a work for research and education. Title 17 United States Code Section 107 lists the various purposes for which the use of copyrighted material can be used "fairly." The law specifies that a copyrighted work can be used without permission for the following purposes:

Criticism and comment

Parody and satire

Scholarship and research

News reporting

Teaching

Take Action: Copyright Tips

- Obtain written permission from copyright owners
- Check the terms and conditions of use or copyright information before downloading material from a website
- Obtain music, video games and other software from legal download sites
- Obtain a copyright for material that you have authored
- Do not assume that works that are in public domain are not copyrighted
- Avoid downloading free screen savers, free-ware or shareware applications

Review the UHS policy on the Digital Millennium Copyright Act

What is the GLB Act?

The Gramm-Leach-Bliley Act (also known as the GLB Act) is a federal law which mandates that financial institutions, including institutions or higher education, protect the security, confidentiality and integrity of customer information 16 CFR 314.1 (a)

GLBA

Gramm/Leach/Bliley Act

What does the GLB Act require?

Mandates the University of Houston System, its component universities and employees safeguard financial information that is collected or maintained in connection with its financial institution activities.

GLBA
Gramm/Leach/Bliley Act

The University of Houston System and its component universities must protect financial information in paper, electronic and other forms.

What is Customer Information?

"Any record containing nonpublic personal information … about a customer of a financial institution, whether in paper, electronic or other form that is handled or maintained by or on behalf of (the University of Houston System, its component universities or its affiliates)." 16 CFR 314.2 (b)

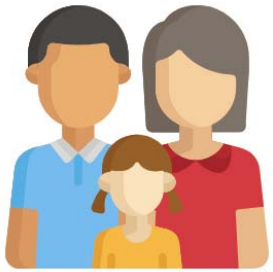
"All financial information in the possession of the University of Houston System and its component universities must be safeguarded regardless of whether such information pertains to individuals with whom (the University of Houston System and its component universities have) a customer relationship, or pertains to the customers of other financial institutions that have provided such information to (another financial institution)." 16 CFR 314.1 (b)

GLB Act Individuals Protected

Individuals protected include:

Applicants

Students



Parents / Guardians

Employers

Donors

GLB Act

What type of information must be safeguarded?

Credit card account numbers

Bank account numbers

Income histories

Credit histories

Social Security numbers

GLB Act

What are the potential risks of not safeguarding information?

- Unauthorized access of financial information by third parties
- Unauthorized transfer of data to third parties
- Interception of data during transmission
- Physical loss of data due to disaster or theft
- Compromise of computer system security

GLB Act:

How should customer information be safeguarded?

The Federal Trade Commission (FTC)
Suggestions for safeguarding information:

- Check references before hiring new employees
- Use password protected screen savers
- Change passwords frequently
- Install anti-virus software that updates automatically, change passwords frequently
- Regularly check with software vendors to install patches that correct software vulnerabilities
- Backup all customer information regularly
- Caution customers against transmitting sensitive financial information via electronic mail
- Encrypt and password protect sensitive customer information if it must be emailed

GLB Act:

How should customer information be safeguarded?

The Federal Trade Commission (FTC)
Suggestions for safeguarding information:

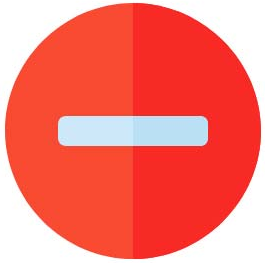
- Combine passwords and personal identifiers to authenticate the identity of customers
- Store sensitive printed materials and electronic records in a locked and secure area
- Ensure that storage areas are protected against flood and fire
- Shred customer information and store it in a secure area until it is discarded
- Delete all customers information from computers, disks, hard drives and other media and store them in a secure area until they are discarded
- Destroy all hardware that is to be discarded

For more information on how to safeguard information, please see the FTC's website:

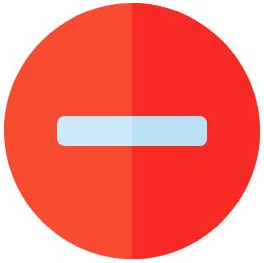
http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm

GLB Act

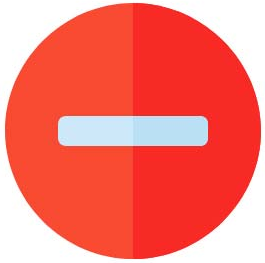
Who do I contact if I do not know what to do?



It is important to recognize fraudulent attempts to obtain customer information

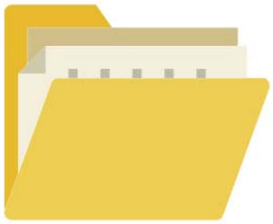


If you receive a request for a customer's financial information, refer the requestor to employees who have undergone information security training



If you suspect an attempt to fraudulently obtain a customer's financial information, immediately report the attempt to your supervisor who should then report the attempt to the Information Security Program Coordinator / Information Security Officer (ISO)

Health Insurance Portability and Accountability Act (HIPAA) & Texas Medical Record Privacy Laws



Ensures the confidentiality and integrity of protected health information that an employee or component receives, creates, collects, transmits and/or maintains

Protects such health information from reasonably anticipated threats, uses and disclosures

Individuals whose job requires specific HIPAA trainings will receive this training at their departments

Let's see what you've learned!

Quiz

Thank you for completing

SECURE OUR SYSTEMS

UNIVERSITY of HOUSTON