University of Houston System
Identity Theft Prevention Program
Fiscal Year 2025

Sergio Leal
System-Wide Compliance Officer
October 31, 2025

University of Houston System
Identity Theft Prevention Program
Executive Summary
Fiscal Year 2025

Board of Regents Policy 42.02, Identity Theft Prevention Program, requires the system-wide compliance officer to annually prepare an executive summary of all activities of the Identity Theft Prevention Programs of the component institutions (Audit and Compliance Committee Planner, Item 5.06). Listed below are the reports from each university.

University of Houston and UH System Administration

All UH and UHS Administration employees and students receive automated email messages whenever there is a change in the University database to their bank account information, email address, home address, or W-4 withholding. The email instructs the recipient to contact UHS Information Security if they did not initiate this change. UHS Information Security investigates all reports.

The University of Houston entered into a multi-year contract with JBC Inc., DBA Skelton Business Equipment, which is an authorized Sharp distributor, for copier service, following RFP process. Skelton has configured all UH copiers to immediately erase images on the hard drive after each job

In Fiscal Year 2025, UHS credit card merchants (i.e., UHS departments that accept credit cards) completed the required Payment Card Industry (PCI) compliance surveys and all were compliant based on the standards set by the credit card payment industry. The major thrust of PCI standards is the protection of personal identifying information and prevention of fraud for merchants that accept credit cards. UHS merchant employees are required to complete annual training to refresh their knowledge of PCI standards so that credit card information is protected

UHS Information Security maintains standards for UHS email distribution, so that email recipients can more easily distinguish between legitimate email and illegitimate (phishing) email that is designed to obtain personal information. UHS Information Security uses enhanced email technology solutions designed to detect and block malicious emails including phishing and impersonation messages. Email encryption is available to all UHS users to protect Level 1 data.

All UHS universities use multi-factor authentication for all faculty, staff and students.

During October-November, 2025, all UH departments with “covered accounts,” as defined by the Federal Trade Commission’s Red Flag Rules, completed their twelfth annual web training to provide appropriate department personnel with an overview of the requirements for securing personal identifying information. Each of these departments developed identity theft prevention procedures tailored to their operation.

University of Houston-Clear Lake

All University of Houston-Clear Lake(UHCL) employees and students receive automated email messages whenever there is a change in the University database to their bank account information, email address, home address, or W-4 withholding. The email instructs the recipient to contact UHS Information Security if they did not initiate this change. UHS Information Security investigates all reports.

UHS Information Security maintains standards for UHCL email distribution, so that email recipients can more easily distinguish between legitimate email and illegitimate (phishing) email that is designed to obtain personal information. UHS Information Security uses enhanced email technology solutions designed to detect and block malicious emails including phishing and impersonation messages. Email encryption is available to all UHCL users to protect Level 1 data.

UHCL also mandates using multi-factor authentication (MFA) for critical University services accessed by faculty, staff, and students. This additional layer of authentication significantly reduces the risk of unauthorized access and helps ensure that sensitive institutional and personal data remain protected against cybersecurity threats.

University of Houston-Downtown (UHD)

All UHD employees and students receive automated email messages whenever there is a change in the University database to their bank account information, email address, home address, or W-4 withholding. The email instructs the recipient to contact UHS Information Security if they did not initiate this change. UHS Information Security investigates all reports.

During Fiscal Year 2025, UHD reconfirmed it is in compliance with Payment Card Industry (PCI) standards. The primary purpose of PCI standards is the protection of personal identifying information and the prevention of fraud for merchants that accept credit cards. UHD reported compliance with the new, updated, and more detailed standards on 10 separate Merchant Accounts.

Throughout the year, the Student Business Services department performs spot checks of the protocols that are in place to ensure employees do not inadvertently disclose a student’s personal information. These protocols include actions such as shielding computer screens so no one can see them except the user and prohibiting the discussion of student account information without positive identification of the student.

UHS Information Security maintains standards for UHD email distribution so that email recipients can more easily distinguish between legitimate email and illegitimate (phishing) email that is designed to obtain personal information. UHS Information Security uses enhanced email technology solutions designed to detect and block malicious emails including phishing and impersonation messages. Email encryption is available to all UHD users to protect Level 1 data.

UHD uses multi-factor authentication for all faculty, staff, and students.

During the system-wide Fiscal Year 2025 mandatory training period, October – November 2025, UHD employees working in departments that manage “covered accounts” that could be subject to identity theft, completed the UH-System Red Flag Rules mandatory training. Additionally, many of these same employees must take and pass training courses in Family Educational Rights and Privacy Act (FERPA), Fraud Awareness and Credit Card Information Security. These employees are scheduled to complete the same training during the October – November 2025 timeframe. The purpose of this training is to provide appropriate department personnel with an overview of the requirements for securing personal identifying information.