University of Houston System
Identity Theft Prevention Program
FY 2023

Phillip W Hurd

Phillip W. Hurd
Chief Audit Executive
October 31, 2023

University of Houston System
Identity Theft Prevention Program
Executive Summary
FY 2023

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.

UHS Information Security utilizes Tenable software to locate certain types of UHS defined Level 1 data, including personally identifiable information, on institutional devices and assists users with removing or protecting Level 1 data where it is located.

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 FY 2023, all 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 UH email distribution, so that email recipients can more easily distinguish between legitimate email and illegitimate (phishing) email that is designed to obtain personal information. UH uses enhanced email technology solutions designed to detect and block malicious emails including phishing and impersonation messages. Email encryption is available to all UH users to protect Level 1 data.

UH uses multi-factor authentication (DUO) on critical services for all faculty, staff and students.

During October-November, 2022, all UH departments with “covered accounts,” as defined by the Federal Trade Commission’s Red Flag Rules, completed their eleventh 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 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 utilizes Tenable software to locate certain types of UHS defined Level 1 data, including personally identifiable information, on institutional devices and assists users with removing or protecting Level 1 data where it is located.

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. UHCL 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 uses multi-factor authentication (DUO) on critical services for all faculty, staff and students.

University of Houston-Downtown

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 FY 2023 UHD reconfirmed its 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.

Student Business Services conducts periodic checks throughout the year to verify the effectiveness of the protocols in preventing unintentional disclosure of a student’s personal information. These measures involve activities such as adjusting computer screens to restrict visibility to the user and prohibiting any discussion of student account information without positive student identification.

UHS Information Security utilizes Tenable software to locate certain types of UHS defined Level 1 data, including personally identifiable information, on institutional devices and assists users with removing or protecting Level 1 data where it is located.

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. UHD 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 (DUO) on critical services for all faculty, staff and students.

During the system-wide FY 2023 mandatory training period, October – November 2023, 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 2023 timeframe. The purpose of this training is to provide appropriate department personnel with an overview of the requirements for securing personal identifying information.

University of Houston-Victoria

In FY 2023, there were no known reports of confirmed identity theft fraud or the unauthorized compromise of financial or other privileged information involving students or employees. Registrar and Student Records, Financial Aid, Human Resources, Student Billing, Student Life & Services, Information Technology, and the Academic Schools Online Support Technicians participate in the UHV Identity Theft Program. The UHV program includes departments that oversee covered accounts as well as departments involved in operations where there is a reasonable likelihood that identity theft could occur.

General program oversight of the campus program, including implementing and updating the campus identity theft program as described in UHV Policy A-27, continues to be the responsibility of a Program Administrative Group comprised of the Campus Compliance Officer (Program Administrator), Bursar, Information Security Officer, and the Human Resources Director.

All UHV 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 W4 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 utilizes Tenable software to locate certain types of UHS-defined Level 1 data, including personally identifiable information, on institutional devices and assists users with removing or protecting Level 1 data where it is located.

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

UHV uses multi-factor authentication (DUO) on critical services for all faculty, staff, and students.

UHV FY 2023 Awareness and Prevention Activities:

- The Registrar and Student Records department sends Student Listserv email notices at the start of the fall and spring semesters informing students of the campus Identity Theft Program.

- When changes were made to employees' and students' email or mailing addresses, they received automatic email notifications through the HRMS database confirming the change. University employees also received notifications when changes were made to W-4 and insurance information, or direct deposit information changes were made to their personal accounts.

- Admissions and Student Recruitment, Financial Aid, Student Life and Services, Human Resources, Student Billing and Student Records, and Online Academic Technicians departments have protocols in place to help verify identity and prevent the unauthorized release of financial or other confidential personal information. These areas have been instructed to review their written protocols annually.