Memo to Users Regarding Elevated Access Privileges and Protection of University Systems

In an effort to ensure proper protection of university systems regularly providing users with elevated access privileges within PeopleSoft, the following memo will be sent to faculty and staff meeting the criteria noted below the message.

Dear <Insert Name Here>:

We have identified that your UHS PeopleSoft account has elevated access privileges based on your job duties. This means that you have been granted the ability to access and modify UHS organizational financial asset information or information belonging to other UHS faculty, staff and students. As a result, you are responsible for ensuring that your account and all of the devices you use to access UHS resources with your account must meet the following security standards:

1. You must safeguard your account information at all time. Your PeopleSoft password should be a strong password. It should be unique and not re-used on any non-UHS site. For more information on strong passwords and account best practices please see the UHS IT Security website.
2. All of the computers and devices you use to access PeopleSoft must be securely maintained. It is your responsibility to verify the following:
    a. All software is updated and kept current with all patches. This includes: the operating system, applications and anti-virus/anti-malware software.
    b. The computer is configured for regular virus scanning.
    c. UHS Peoplesoft data is not stored on personally-owned devices unless specific prior approval has been granted.
    d. On your UHS-issued computers, you have Identity Finder installed and run reports on a regular basis. Sensitive information discovered is immediately addressed and handled according to university policies regarding data protection.

Your Information Security Officer will be following-up with you to answer any of your questions regarding securely maintaining your devices and verifying that your UHS-issued computers meet all of the requirements listed above.

We appreciate all of your diligence in protecting university data through these safeguarding efforts, and are happy to assist you in these endeavors if necessary.

Mary E. Dickerson, MBA, CISSP, CISM, PMP
Executive Director, IT Security
Chief Information Security Officer
University of Houston | University of Houston System
A Carnegie-designated Tier One public research university
phone: 832-842-4679
email: mdickerson@uh.edu

Elevated Access Definition

PeopleSoft users who have administrative page access to view and change FERPA and Privacy related information for faculty, staff, and students; and organizational financial asset information.

FERPA and Privacy PeopleSoft Data Elements:

- Date of Birth
- Social Security Number
- Direct Deposit
- W4 Federal Tax
- Email Address
- Home Mailing Address
- Home Phone Number
- Student Grades
- Student Transcripts & Records
- Student Financials
- UH System Finance & Budget Program

Roles to Identify Elevated Access

- UHS_ADMIN_USER – PeopleSoft HR and Campus Solutions users who have the PS HR/CS icon within the AccessUH portal
- UHS_FINANCE_USER – PeopleSoft Financials application users who have PS Financials icon within the AccessUH portal
- UHM_CS_INSTRUCTOR, UHC_CS_INSTRUCTOR, UHV_CS_INSTRUCTOR

***NOTE: Individuals may be assigned multiple elevated access roles. For example a user may be an employee with elevated access in HR, in Finance, and also may be an Instructor for one of the campuses.**

Out-of-scope Employees who have PeopleSoft access

- Employees who only have access to PeopleSoft PASS site icon within AccessUH portal
  Example: Facilities personnel