College/Division Administrator Meeting Minutes
April 11, 2013

Joshua Menefee, Financial Aid Program Coordinator

New Scholarship Award Memo Process

- All Scholarship Award Memos for FY14 must be submitted electronically to a Sharepoint email address (SFASAMemo@share.uh.edu) as an attachment.
- The attachment must have a unique name without spaces (e.g., Shasta_Bucks_1.25.13).
- The subject of the email should be the name of the department.
- College/Division Administrators should send Joshua Menefee (jjmenefee@uh.edu) a list of employees (name and email address) who can submit Scholarship Award Memos.
- The following documents are attached with the minutes:
    - Scholarship Award Memo Workshop
    - Single Award Memo Template
    - Multiple Award Memo Template
    - Competitive Scholarship Waiver Form

Maria Honey, Assistant Director, Marketing and Communications

MySafeCampus Communication Plan

- MySafeCampus is the anonymous reporting hotline anyone can use to report suspected fraud, non-compliance, or safety concerns.
- Reports can be made online at www.mysafecampus.com or by calling 1-800-716-9007.
- A link to MySafeCampus is posted on the main UH web page, as well as several other UH web pages, and included in annual Fraud Awareness training completed by all UH employees.
- In order to increase awareness about MySafeCampus, Administration and Finance is planning a marketing and communication program, which includes (but not limited to) the distribution of posters and two-sided flyers.
- A&F is waiting to see if the Chancellor plans to issue another communication about MySafeCampus in the near future (similar to November 2011). If so, A&F will do most of its communication following the Chancellor's message to build on that momentum. If not, A&F will proceed with the marketing and communication program.
- Maria will speak to the Dean of Students about whether there is a preference for students to use MySafeCampus to report incidents or another mechanism that is already setup for student reports.
- The following documents are attached with the minutes:
    - MySafeCampus Poster
    - MySafeCampus Flyer

Mary Dickerson, Executive Director, IT Security
Robbi Puryear, Assistant Treasurer

PCI Compliance Issues

- All 113 UH System credit card merchants (i.e., departments that accept payment via credit card) recently completed their annual PCI (Payment Card Industry) survey. However, it is evident from the surveys that some merchants don't fully understand their business process.
- Treasury is working with Internal Audit to develop an audit program to review PCI business processes that will help ensure PCI compliance.

- Any business process changes involving credit cards must be communicated to Robbi Puryear in Treasury before they occur. Treasury will consult with University Information Technology, if needed, but the first point of contact is Treasury.
- Fines for non-compliance with PCI standards start at $50,000 a day per incident.
- Treasury can provide a workshop for credit card merchants to help them understand how to complete future PCI surveys, but Treasury cannot complete the surveys for the merchants.
- Treasury will issue a Request for Proposals for a PCI survey company for FY15 and beyond. We will continue to use the current company for FY14 surveys.

UHS Merchant Use of Third Party Vendors

- Some departments have asked about using a website called "Eventbrite" for credit card processing. Departments should not use Eventbrite because it is not in compliance with the UH System/Bank of America contract.
- All third party vendors must be vetted through Treasury before a credit card merchant decides to use them.

Mary Dickerson, Executive Director, UIT Security

Increases in Spam/Phishing

- In the past two weeks, the average number of spam/phishing emails received by UH has increased from 1.5 million per day to 1.5 million per hour. Other US universities have seen a similar increase.
- UIT Security has a vendor-supported program that rates all incoming email in one of the following categories:
    - Good – goes to email
    - Possibly bad – goes to spam folder
    - Probably bad – goes to quarantine and employee later receives an email with a list of quarantined email
    - Bad – goes away (employee never sees it)
- UIT is working with the vendor and other universities to see if more email can go to quarantine instead of to the spam folder.
- Phishing emails, in which people are tricked into clicking on a link that downloads malware or providing personal information, are becoming more sophisticated. Creators of phishing email do research on the intended victim to personalize the email so that it seems legitimate. University administrators are targets too, so all staff should be alert to these emails.
- Some people receive "undeliverable messages" even though they did not send email to the address indicated. This is because someone is spoofing UH email addresses. It does not mean that someone has breached your email.
- Reporting any questions or concerns about email security to UIT Security to security@uh.edu

Level 1 Data Protection Concerns

- Level 1 data is confidential, sensitive, or mission critical data, which includes (but not limited to) social security numbers, driver license numbers, bank account numbers, full credit card numbers, medical records, and some student records.

- Level 1 data may be stored on a university server but may not be stored on flash drives, laptops, or other portable devices.
- Level 1 data must be protected with access controls (passwords), may not be sent by unencrypted email, and may not be stored on a non-university device unless there is a valid business reason that has been pre-approved.
- See the attached explanation of the three levels of data, which is covered in new employee orientation.

Results of Campus ISO Compliance Survey

- Sixty (60) UH Information Security Officers completed a Compliance Survey in January 2013.
- Some of the issues mentioned include:
    - UIT Security will scan department websites and provide feedback at no charge. Contact UIT Security at security@uh.edu if you would like this service.
    - Some vendors support single sign-on using your Cougarnet user ID and password, which is preferable to requiring a separate user ID and password.
    - Each department must have its own incident response plan (MAPP requirement). If there is nothing different or unique about the department (unlikely), the department can utilize the UIT incident response plan instead.
    - It is important to keep software patches current. Not applying patches provides an opportunity for hackers to gain personal information. Some departments push software updates out to their users electronically, which makes updates easier to maintain.
- Contact Mary at medickerson@central.uh.edu if you want specific information about your college/division's response to the survey.
- See the attached ISO Survey Results for an overview of the results.

College/Division ISO Engagement

- Mary asked the College/Division Administrators to encourage their Information Security Officers to attend the monthly ISO meetings, which provide training and information to the ISOs. In addition, the ISOs can voice their opinion about proposed changes to IT policies or procedures.
- Mary will provide a quarterly report to each College/Division Administrator to let them know whether their ISO is attending the meetings.
- There are three requirements to be considered a "Certified ISO":
    - Appointed by the College/Division Administrator as a security officer
    - Attend a workshop offered by IT
    - Complete formal security training (either at UH or off-campus)
- See the attached list of current Certified ISOs and an overview of the ISO program.

Margaret Busch, Payroll Manager, Human Resources
Joan Nelson, Executive Director, Human Resources

Weekly Payroll Encumbrances

- Payroll is testing a process to apply weekly payroll encumbrance updates to the Finance System, which they hope to implement soon. Finance will be involved in the testing too.

- Currently, payroll encumbrances are updated only on each payroll "on-cycle," which is once a month for monthly employees and once every two weeks for bi-weekly employees.
- Contract Margaret Busch regarding questions at mbusch@central.uh.edu

Termination Checklist

- HR is working with UIT to automate the termination checklist, so that employees leaving UH don't have to walk around to various offices to receive verification that the employee does not have university assets/access or outstanding debt.
- Buildings will be converted from key access to card reader access, so that access can be removed when an employee leaves.
- The goal is for terminating employees to see everything that is outstanding in PASS, and for the clearance of these items to be completed through electronic workflow.
- Joan will ask some College/Division Administrators to participate in focus group.

Mike Glisson, Controller

Digital Signatures vs. Signature Capture Devices

- Signature capture devices are like the devices at grocery stores where you sign for a credit card purchase. You point your mouse on the electronic document (PDF, Word, or Excel) where you want to sign and sign the signature capture device that is connected to your computer. Your signature appears on the electronic document. Some colleges/divisions have been using these devices for the past couple of years.
- Digital signatures, on the other hand, are electronic signatures that contain the date and time stamp of the person who signed the document and provide some authentication of the signer's identity. The State of Texas currently approves of only four vendors who offer digital signature solutions. UH has contracted with one of those vendors.
- On March 28, Mike with Mary Dickerson, UIT Security, Mark Yzaguirre, Contracts Administration, and Russ Hoskens, Internal Audit, to discuss when signature capture devices may be used. They concluded that signature capture devices may be used for any documents where a scanned signature is acceptable.
- Digital signatures delivered by Adobe are not permitted by state law and should not be used.
- The Digital Signature Committee will focus on applying digital signatures (approved by the state) to those documents where it is necessary to verify the identity of the signer.
- Mike will send an email to the administrators with additional guidance and information.

Office Supply RFP

- The seven year office supply contract with Today's Business Solutions ends on August 31, 2013.
- UH has issued a RFP and will issue a new contract for office supplies starting September 1, 2013.
- UH departments should continue to use Today's Business Solutions for all of their office supply purchases through August 31, 2013.

Xerox Copier Contract

- UH plans to exercise the three year extension of the Xerox copier contract to August 31, 2016. Xerox has been the UH copier vendor since September 1, 2010.

- Some administrators expressed concerns over Xerox copier performance and/or sales support, while others said they were pleased.
- Departments that were leasing a Xerox copier prior to September 2010 continue to be supported by Xerox corporate sales (Jeff Parks), while departments that were leasing other copiers are supported by Xerowgraphics (Shawn Greer), which is a distributor of Xerox copiers.
- Contact Mike Glisson at 713-743-8706 if you have any concerns about Xerox service or performance.