

College/Division Administrator Meeting Minutes
October 13, 2011

Susan Nester, Director, Compensation/HRMS

ePerformance Technical Issues

HRMS made the following enhancements to ePerformance:

- Mission and Initiatives are hidden, but available through a link on the ePerformance evaluation page, so that the evaluation page is shorter.
- Ratings now show two digits to the right of the decimal, instead of one. The “Ratings” link explains that ratings of .80 and higher round up and ratings of .79 and lower round down to determine the performance category (Generally Meets Expectations, Exceeds Expectations, etc.).
- A warning message displays if the weights for an evaluation category (Goals, Responsibilities, etc.) or the sum of all categories do not total to 100%. However, you can still save your answers in case you need to complete the weights or evaluation later.
- An error message displays if you click on “submit” and the weights do not equal 100% because you cannot submit an evaluation unless the weights of each evaluation category and the total of all categories equal 100%.

Calendar Year 2010 ePerformance Statistics

- 54% completed and submitted to HR
- 28% completed but not submitted to HR
- 18% not completed (weights and/or evaluation not completed)

See Susan’s October 11 email with instructions for running the EPM Document Status Report in the HR System, which indicates the status of ePerformance documents not completed. Susan asked the CDAs to encourage faculty and staff in their college/division to complete and submit the remaining 2010 ePerformance documents.

Calendar Year 2011 ePerformance Information and Enhancements

- Deadline for completing 2011 criteria is December 15, 2011.
- 2010 employee and manager responsibilities will be copied to 2011 if the employee is in the same job code and position. Responsibilities can be deleted or added, if desired, by sending an email to HRMS.
- Deadline for managers to submit their 2011 evaluations to HR is March 1, 2012.
- There may be a merit pool for FY13 and in order to be eligible for merit the employee’s ePerformance evaluation for calendar year 2011 must be submitted to HR.
- In addition, if the manager does not submit all of his/her evaluations to HR, he/she will not be eligible for merit, which will be added to an HR policy.
- HRMS will create a report that CDAs can use to manage merit for FY13, if offered.
- Managers must rate all evaluation criteria, including criteria with a weight of zero. Alternatively, managers can delete evaluation criteria with a weight of zero if they don’t want to rate it. Either way, it will not impact the employee’s performance score.
- HRMS can change the senior manager who reviews the ePerformance evaluation (not the supervisor) if HRMS receives an email approved by the CDA requesting this.
- HRMS is working on allowing attachments to be uploaded to ePerformance, since “Outstanding” and “Needs Improvement” require additional documentation.
- HRMS will develop a flowchart to map the ePerformance process.

College/Division Administrator Meeting Minutes
October 13, 2011

Calendar 2012 ePerformance Criteria

- If 2011 performance criteria is completed by December 15, 2011, the responsibilities and manager responsibilities will automatically roll over to 2012, so the manager will not need to enter them again for 2012.
- If not completed by December 15, 2011, criteria for 2012 should be entered no later than January 31, 2012 so employees know what they will be evaluated on during the 2012 calendar year.

Online Campus Phone Directory

- An online campus phone directory should be available by the end of October, which will include employee and department information.
- HRMS will send the CDAs the department information (phone, fax, URL) and ask them to update or distribute to their DBAs to update.

Sandy Coltharp, Director, Training & Development

ePerformance Training

- Classroom training is still available for ePerformance. Contact your HR Generalist or the HR Training group to request training.

Mandatory Training

- FY12 training has been improved somewhat over previous training to be more engaging and entertaining. HR will continue to make improvements to the training for future years.
- During the first week of training, there were some technical glitches related to automated email notices sent to employees who completed training. One email was supposed to be sent within 24 hours of training completion to notify the employee that their training had been completed, but an email was being sent every day instead. HR worked with technical staff to resolve the issue.
- As of October 11, about 2,400 UH employees had completed their mandatory training.
- Employees who complete their training are eligible for a weekly drawing of gift cards.
- Historically, UH has had the lowest percentage of employees who complete mandatory training in comparison to the other UHS campuses, so Sandy would like for UH to do better this year.
- CDAs can email Sandy to add or remove role-based training for an employee.
- HR will send CDAs a list of employees who have not completed mandatory training on a regular basis until a report can be developed for CDAs to run themselves.

Ann Pino, Manager, Human Resources

ePAR and I-9 Compliance

There are a variety of reasons that it is important to submit ePARs and I-9s timely, including:

- Compliance with federal and state law and UH policy
- Ensure new employees are paid on time and their benefits start when they should
- Delays in pay and benefits hurt UH's credibility with new employees, which could result in a bad reputation for UH making it more difficult for UH to attract top employees

College/Division Administrator Meeting Minutes
October 13, 2011

- UH could be liable employee injuries or illness if benefits do not start on time

The following actions are being taken to improve ePAR and I-9 compliance:

- HR will create focus groups to get new ideas on how departments can improve compliance, and will ask the CDAs for volunteers to participate in the focus groups.
- HR will send statistics by college/division to the CDAs for review so they can see how their departments are doing.
- ePAR and I-9 compliance will be discussed at Dean's Council to bring it to their attention.

See Ann Pino's handout on ePAR and I-9 compliance for more information.

David Ellis, Executive Director, Financial Reporting

Implementation of 1% Salary Rider to Support ERS Group Insurance

- A rider to the General Appropriations Act, Article IX, Section 18.09, which was passed by the 82nd Legislature in 2011, increased the employer contribution to the Employees Retirement System (ERS) for group health insurance.
- Beginning September 1, 2011, all state agencies and universities must pay an additional 1% of total base wages and salaries for all benefits eligible employees to ERS regardless of funding source.
- The Comptroller issued guidelines for these payments in the last week of September.
- This applies to all benefits eligible employees, except those that are "not enrolled" in health insurance (about 40 employees system-wide).
- For salary paid with local funds, the 1% expense will be calculated at the end of each accounting period (month) and applied to the department's local fund cost center under account 51126.
- For salary paid with state funds, the 1% expense will be calculated at the end of each period and applied to an institutional cost center under account 51126, just as other benefits for salary paid with state funds are applied to institutional cost centers.
- See David's handout for a summary of this requirement and report by college/division of the amount charged for September 2011 (actual) and for FY12 (estimated).
- The 1% expense will not appear on the Labor Distribution Report, just like Unemployment Compensation Insurance (UCI) and Workman's Compensation Insurance (WCI) do not appear on the report.
- Payroll reallocations do not need to include account 51126. The expense will be moved automatically (like UCI and WCI) based on whether the base salary in the cost center increased or decreased during the month.
- The 1% expense will be in effect for FY12 and FY13, but may go away in FY14 if ERS raises its rates for employer contribution to compensate.
- Drs. Carlucci and Bose are expected to send a letter announcing this change to the campus.
- If a CDA would like more detailed information about the allocation of expense (by department or employee), please contact David at dellis@central.uh.edu.

Mary Dickerson, Executive Director, Information Technology Security
National Cyber Security Awareness Month and Related Activities

October Activities

- October is National Cyber Security Awareness Month, during which UH Information Technology (UIT) has planned several activities to promote computer security awareness.
- UIT's theme is "Be a Curious Cougar" to encourage students and employees to ask questions when they see something they are unsure about or that does not seem right.
- UIT is promoting cyber security through blogs, Facebook and Twitter tips, workshops, and department presentations.
- Workshops are also "Cougar Trading Card" events, in which students can collect cards to redeem for scholarships, which is intended to encourage student participation. More information about Cougar Trading Cards is available at: <http://www.uh.edu/tradingcards/> and at <http://www.uh.edu/sfac/requests/additional/UC-UC%20Satellite%20FY%202011-12%20Base%20Augmentation%20Request%20Cougar%20Trading%20Cards.pdf>
- In addition, code words are given at the end of UIT presentations and in the blogs, which can be emailed to UIT to be included in a drawing for a prize.
- Mary handed out lanyards (used to hold ID badges) to remind everyone to be "safe, simple, and secure." DBAs can contact Mary at medickerson@central.uh.edu if would like some lanyards for their department.

Phishing Emails

- "Phishing" emails are email blasts to large groups of people designed to steal personal information, while "spear phishing" is targeted to specific individuals (usually upper management) to steal their information.
- Though spear phishing is a bigger problem in the corporate world, university administrators should be aware that they and the people they support may receive this type of email too.
- Do not reply to email requests for personal or financial information.
- Do not open attachments or click on links in an email unless you know the person who sent it.
- Manually enter the website address in your browser, rather than click on an unknown link. You can also hover over the link with your mouse to see if the website is a UH address or not.
- Forward suspicious email to UIT Security (security@uh.edu) for review.

UHSecure Wireless Network

- UH students and employees can use the UHSecure wireless network to protect themselves from hackers and identity thieves. If they use the regular (unsecure) wireless network, anyone with the right equipment can record their keystrokes and steal their passwords.
- Anyone with a Cougarnet account can go to www.uh.edu/uhsecure to automatically configure their laptop to use the UHSecure wireless network.

College/Division Administrator Meeting Minutes
October 13, 2011

See Mary's handouts for a list of events related to Cyber Security Awareness Month, a list of UIT Security workshops, security best practices for staff, general security tips, security tips for social networking, tips on recognizing phisher email, and using the UHSecure wireless network.

MAPP 10.05.03, Data Classification and Protection

This MAPP, which was approved September 6, 2011, identifies three levels of data and the security requirements for each:

- Level 1 Data: Confidential information, sensitive personal information, and mission-critical information. Level 1 data must be stored on a "critical information resource" (see MAPP for definition) and contain appropriate access controls (user ID and password or locked filing cabinet). Also, level 1 data cannot be transmitted via wireless network or email, unless encrypted, and cannot be stored on a removable or portable device (laptop or flash drive), unless encrypted, or on a non-university device, unless specific advanced permission has been obtained from the department head or Chief Information Security Officer.
- Level 2 Data: Public data that is not in the public domain yet, such as a professor's lecture notes before the lecture is given. UIT recommends storing level 2 data on a critical information resource and that they contain appropriate access controls, though this is not required.
- Level 3 Data: Public data in the public domain, such as the UH website. No protection needed.

Different people have different responsibilities when it comes to protecting data:

- Information owner – Classifies data into the appropriate level.
- Information custodian – Ensures safeguards are in place.
- Information user – Knows where the data is stored.

Identity Finder software can help departments identify and protect or remove some level 1 confidential and sensitive personal information, such as social security numbers and credit card numbers. About 30% of departments have scanned their computers with Identity Finder so far. The goal is for all UH departments to scan their computers by December 31, 2011.

MAPP 10.05.03 is at: <http://www.uh.edu/af/universityservices/policies/mapp/10/100503.pdf>

Upcoming Information Security Officer (ISO) Workshops

About 80% of UH ISOs have received the required training. The remaining 20% can sign up for ISO workshops to be held on October 19, 2011.

Single Logon through Portal

- By January 2012, UIT hopes to provide a uniform login page to a portal for all UH systems, including Housing, Parking, PeopleSoft, etc.
- You will use your PeopleSoft or CougarNet user ID and password to login.
- The portal will not only be more convenient, but more secure than logging into multiple systems.

College/Division Administrator Meeting Minutes
October 13, 2011

- The challenge is trying to integrate the various departmental systems on campus into the portal.

Contact Mary Dickerson at medickerson@central.uh.edu if your department needs help or would like a presentation on any of the above topics.

David Johnson, Executive Director, Technology Services and Support

Technology Support Services FY12 Service Update

Technology Support Services lost 17 positions due to budget cuts. However, David has strategically reorganized TSS to be more responsive to customer needs. Highlights of some changes are as follows:

- Dedicated trainers have been replaced with subject matter experts, who will provide more targeted (granular) training to address specific needs through online and classroom courses.
- The Technical Partners Program is now managed by David to better coordinate user support across campus.
- The hours for the Technology Commons Computer Lab have been reduced due to security concerns. Most students used the lab to print documents. David is conducting a study to see if there are more secure and convenient locations that students can use for printing.
- Laptop checkout at the computer lab is now for 12 hours maximum, instead of the indefinite period checked out previously.
- Process improvements were made to network operations that reduced workflow from 62 to 8 steps. Also, network zones were “softened” so that support staff can cover someone else’s zone if the assigned person is out.
- TSS is working with Purchasing to ensure we get the best deal possible on IT purchases by leveraging the purchasing power of the UH System, the campus, or a college/division when possible.
- Information Technology Availability Center (ITAC), which monitors and responds to system outages, now reports to David, which should provide increased communication and coordination between ITAC and TSS.

Joe Mendez, Director, Emergency Management

Kelly Boysen, Specialist, Emergency Management

Emergency Management: Key Components

The mission of Emergency Management is to:

- Prevent/mitigate
- Prepare for
- Respond to and
- Recover from disasters and other emergencies.

The PIER communication system includes the following types of notices regarding emergencies:

- General Notification – generate awareness about a possible threat to UH (e.g., tropical storm that may affect UH)
 - Email to certain emergency personnel at UH

College/Division Administrator Meeting Minutes
October 13, 2011

- Post on UH emergency website (www.uh.edu/emergency)
- Advisory – addresses a more serious threat but still uncertain how or whether it will affect UH (e.g., category 1 hurricane, tornado, etc.)
 - Email to all UH students and employees
 - Post on UH emergency website
 - Social media (Facebook and Twitter)
- Alert – addresses a serious threat that is imminent/actualized that requires immediate action (approaching hurricane, active shooter, unknown or uncontrolled chemical release, tornado damage to campus, etc.)
 - Email, phone, and text via PIER
 - UH main web page (www.uh.edu)
 - Social media (Facebook and Twitter)
 - UH sirens
 - Alert beacons
 - Police door to door

In the event of an Alert, people should know whether to:

- Evacuate,
- Shelter-in-place, or
- Lock-down

Everyone should update their contact information at <https://myuh.uh.edu> so they can receive email, phone, and text messages in the event of an emergency.

Departments should create and regularly update a phone tree of employee home/cell phone numbers and conduct monthly drills for evacuation and emergency response.

See Joe's presentation for more information.

Contact Joe (jmendez3@central.uh.edu) or Kelly (krboysen@central.uh.edu) if you would like emergency training for your department.