College/Division Administrator Meeting
Room 302, Melcher Hall
February 13, 2020 - 9 AM to 11 AM

Meeting Minutes

Courtney Stein, Wellness and Engagement Programs Administrator

Wellness Initiative

- HR's Power Up program is to provide information on programs and support for health and wellness initiatives
- The purpose is to increase health and productivity and to lower absenteeism and costs.
- 2020 initiatives are:
    - Best Bite calendars, which have wellness tips, recipes, and other suggestions
        - Email Courtney Stein with your mail code and how many you need for your department
    - Biometric Scanning – HR is working to have BCBS Texas come and do scans of people for things like diabetes, cholesterol, and body mass indexing
    - Mobile Mammography – this year there will be three days offered
    - Fitness Release time – updated policies allow ½ hour three times per week
        - Application is only required in the spring of each year
        - Release time cannot coincide with daily start and end times, but can coincide with lunch breaks
    - Employee Wellness Champion Program – this is a new initiative
        - The purpose is to encourage health at work by connecting people to programs
        - Champions can be anyone that wants to be involved
        - Champions will communicate program information, engage people, and encourage people
        - Expectations of Champions are:
            - Have their supervisor's approval to participate
            - Attend an orientation
            - Attend a meeting once a month
            - Spend an additional 1 – 2 hours per month doing things like talking to people, hanging flyers, etc
            - Commit to 2 years of service
        - The goal is to have 1 person in each department.
            - Please identify 1 or 2 people in your area and email their names to powerup@uh.edu

Mary Dickerson, AVC/AVP IT Security

Annual UH Information Security Compliance Survey

- The annual compliance survey will be coming out soon
- The College/Division Information Security Officer (ISO) is responsible for responding
- There are approximately 15 questions about general security and compliance
- The survey is due on May 6th, all areas must respond

Best Practices Resources

- There are many policies, so IT has developed checklists derived from the policies to assist departments in ensuring compliance
- These are not turned in or reviewed, they are designed to provide easy to understand assistance

- There is room for interpretation in some of the requirements, as there is more than one way to do most things. Areas with questions can contact the Information Security Team for assistance.

HB3834 – Awareness Training

- HB3834 requires security awareness training beyond just state agencies – includes municipalities, vendors, and elected/appointed officials
- UH Systems annual "Secure Our Systems" training meets the requirement, so many people will not see a difference
- The change will affect appointed officials (Board of Regents) and certain contractors
- Board of Regents training is being developed
- IT is working with HR on the contractors. Contractors included will be those that have a POI and a cougarnet account. Training will be required at least once during the term of the contract.
    - This is only for contractors with access to university information resources
    - Contractors that only observe people working in our systems will not need to do training.
- The first training will be due by June 1 of this year.
- UH's Secure Our Systems training is certified by the DIR, and UH has offered to share the training with other organizations.

Use of Hosted/Cloud Services

- SAM 07.A.08 – Data Classification and Protection covers the use of cloud or hosted services (where University data is elsewhere located)
- For example – Office 365, which all employees have access to
- The rule for cloud and hosted services is: you must have a contract for these services
    - This is done to protect the University for many purposes – inadvertent release of data, loss of data, unauthorized use of data, to help ensure compliance with FERPA regulations
- Basically, no contract, no data
- Specific program questions that come up:
    - Drop Box – if you have a contract
    - Box – if you have a contract
    - Google Docs – cannot be used because they will not do departmental level agreements and the University does not have an agreement
- We strongly encourage all departments to utilize the services the university already provides – usually free and with campus support available.

Email Access Requests

- When employees leave the University, it is important to have them: 1) turn on an out of office: 2) turn over all email files that you may need; and 3) set up a forwarding address for their email.
- If an employee leaves without doing these things
    - IT can put in an out of office message for them.
    - IT cannot get you access to their email files or have their emails forwarded to you. To obtain this access, the request must be approved by General Counsel and Human Resources, and such requests must be for specific subjects or date ranges. This is due to privacy rules.
- It is much easier to just handle it in advance, as if the employee turns it over or sets up the forwarding it is allowable.
- This does not apply to documents on University owned equipment located in the department, as the employee should have understood that those are University files.

Changes from Audit reports – The following is based on information IT Security received from audit report drafts and preliminary plans to address the findings. All plans will be finalized with campus TM/ISOs when more details are determined.

- Issues found:
  - Old operating systems
  - Lack of asset inventory by IP address for network scans
  - Shared local administrator profiles (same on all machines)
  - Non-current patches
  - Unprotected Level 1 data
  - Domain accounts being added to Administrative groups
  - Legacy protocols that can be easy to exploit
  - Easily compromised passwords
- Phishing/Mail Protections
  - IT is going to utilize a security solution called ProofPoint
  - IT will also be blocking campus outbound SMTP.
    - Department mail servers must be registered or they will not work
  - According to UHS policy – SAM 07.A.07 Employees can only use their UH email address for official business
- Password Management Strategy
  - IT will do an awareness campaign
  - IT will encourage the use of security phrases
  - Passwords will require 12 characters in the future
  - Multifactor authentication will be in place by 8/31/2020
    -
    - There will be several different options for the 2nd factor. Authentication can be sent as a text, by email, by using a hardware key etc.
  - LastPass will be used to manage passwords for multi-account users.
  - MS Local Admin Password Solution (LAPS) will be used to securely manage local administrator passwords.
  - Policies will be updated to reflect these changes
- UH Wireless/UH Secure
  - UH Wireless and UH Secure will be separated
  - UH Wireless will be for guests and will only be able to access web-functions. No authentication will be required.
  - UH Secure will require authentication and be used for logging in to servers, remote desktops and accessing other on-campus information resources.
  - Notifications of the changes will be sent prior to implementation
- Departmental Cameras
  - These cameras are different from security cameras that are managed by UH Police.
  - Departments that use cameras to record space for , observation, research, and other academic purposes need to have the cameras secured
  - Cameras need to use an enterprise IP address, not a public address
  - Cameras need passwords for access, other than the manufacturer default
  - This will help ensure that access is restricted only to those people that should have access
  - If you have such cameras, contact the Information Security team
- Incident Response Policies/Procedures
  - According to university policy, if you detect or suspect that you have had an incident, report it immediately to Information Security
  - Do not try to investigate it yourself – you could interfere with required legal processes or spread the issue
- Campus Vulnerability Management Program
  - Information Security scans the network for vulnerabilities, and also has an outside party scan the network. They are looking for risks like unpatched equipment, outdated machines, etc.

    - When they find machines and systems that pose a risk, they contact the area and request that the issue be corrected.
    - Corrections are to be made in approximately 1 week. After 2 weeks, the issue will be escalated and the item may be removed from the network.
- Enterprise IP Migration Project
    - IT has been reviewing all public IP addresses and determining if they need to be public or if they can be made private
    - The starting point is Dynamically assigned IP addresses; if you are using DHCP, contact Brian Walker for assistance
    - Areas can have a public IP address, but there must be a business justification such as it is a web server
    -
- Spirion (formerly known as Identify Finder)
    - Spirion is used to scan for Level 1 data
    - Spirion will also be used to scan for passwords
    - Spirion must be run at least one time per year, but can be run more often if you are in a high risk area

Elyse Davis, Division Administrator – Business Operations

Internal projects Project End Dates and Accounting End Dates

- DOR has identified that internal awards (I-projects and R-projects) frequently have transactions post after the Project end date.
- In an award, the Project End Date defines the period of performance. Most transactions should occur during this time frame.
- The Accounting End Date defines the time period for final postings and clean up. Few transactions should post during this time frame, and should post close to the beginning of it.
- End dates can be identified in Grants Manager, and also in 1074 and 1063 reports.

Karin Livingston, Controller

- HUB Vendor Fair Announcement
    - Vendor Fair is March 3rd
    - HUB has worked to ensure that vendors that provide desired goods and services will be in attendance
- The May HUB Spot Bid Fair announcement has not been received yet, but it should come soon. All Colleges and Divisions are asked to buy 3 – 5 items.
- Travel workgroup plans
    - We would like to hear comments on issues with the travel process and concur
    - From there we will create a work group to look at travel rules and their reasons to: 1) map what cannot be changed and the reasons why for department use; 2) identify what can be changed and the best changes for the campus; 3) develop training programs to help areas that must approve Travel Requests
- Some changes coming from the SAO Audit:
    - There will be an 18 month (or life of project) limit on emergency procurements
    - All committee members for a solicitation will have to have to take Conflict of Interest and Procurement Training
    - All committee members for a solicitation over $1M will have to complete the SAO Nepotism Form
    - We are working on modifications to the ability to override Late Payment Interest calculations

- Please let me know your thoughts on having some sort of large list of accessible IT to simplify purchasing.