

**Business Administrator Services**

**Forum Minutes**

**October 8, 2014 9:30 a.m. to 11:30 a.m.**

**Kent Student Center Governance Chambers**

**Ron Smith – Training and Development Associate, Human Resources**

**Professional Development Opportunities and Updates**

Ron spoke to the forum about new training programs that have been developed and also reminded the group of ongoing training opportunities available on the HR website.

One of the new programs is **Beyond Compliance**. Within this training module you will find both webinars and some instructor-led sessions on various compliance topics. Beyond Compliance is accessible through MyTraining and the HR website under Training and Development.

Beyond Compliance is an initiative to provide all faculty and staff a minimum of 2 hours of training on the latest standards, policies and laws as it relates to: unlawful discrimination, prevention of harassment or the prevention of violence.

Beyond Compliance is relevant to Kent State University administrative policies, processes or implementation guidelines. All current KSU full time and part-time staff must attend a minimum of two hours of HR compliance training each fiscal year. Full time and part time faculty are also encouraged to meet the training requirement as this initiative benefits all members of the university community.

A **Hiring Certification Program** has also been added. The goal of this program is to enhance KSU hiring procedures regarding compliance, processes and systems. The Hiring Certification program is available to any employee involved in the hiring process. It is a self-paced course used in the Blackboard platform. The certification is good for two years and starts and ends at the start of a fiscal year. Questions or requests for more information on this certification program should be directed to employment@kent.edu or Talent Acquisition at 330-672-2100.

**Workplace Conversations: Maximizing Results** is a new instructor-led four hour workshop building on material from Supervising Successful Performance. This workshop explores methods to successfully conduct a performance improvement conversation. Each participant will assess their competency level, develop performance conversation skills through a seven step model and engage in role play centered around university-specific scenarios. Participants will be asked to complete a one hour follow up after 90 days.

To view and register for online learning, facilitator-led sessions or webinars go to [www.kent.edu/hr/register](http://www.kent.edu/hr/register).

Watch for the following new webinars:

* So, What’s With the Green Dot?
* Step Up and Speak Out
* Beyond Title IX: Supporting Students and Changing Culture Around Power-based Personal Violence
* Managing Your Online Files

Also visit [www.kent.edu/hr/training/e-learning-materials.cfm](http://www.kent.edu/hr/training/e-learning-materials.cfm) to view short online videos that offer a glimpse of workshop content. Content on this website is added regularly.

**Jeff Mori – Assistant Director, UFM**

**University Facilities Management Lock Shop**

Due to the ever changing personnel within departments and the ongoing need for key replacements, Jeff Mori graciously accepted the invitation to meet with the BAS Forum members to review the process for new keys, replacement keys, electronic keys, etc.

In most cases access to buildings, classrooms, offices, storage rooms, etc. are designated by the individual department or building curator. For security purposes key ownership and access should be documented, monitored and reviewed. Upon retirement, resignation or termination of an employee, all hard keys and electronic key cards should be collected and documented accordingly. All keys and cards are to be returned to the Lockshop for repurposing or destroying.

Generally speaking there is a two day turn-a-round for locksmith services. With that said, we must all understand that the beginning of each semester is a high volume period and proper planning can eliminate panic situations.

Regardless of the key type that you are requesting, you must start with the completion of a work order. Access to the work order can be obtained by signing into FlashLine, My Action Items then FlashTrack located in the FAMIS Resources. (Complete instructions can be found at [www.kent.edu/ufm](http://www.kent.edu/ufm).) Every hard key or key card is assigned; you must include names and Banner IDs when requesting cards.

Electronic key card requests must also include an Electronic Lock Form. This form must be completed in its entirety and scanned/emailed to lockshop@kent.edu or faxed to 330-672-7843.

All keys, whether hard key or electronic key card, must be picked up from the UFM Lock Shop which is located at 1787 Summit Street. Pick up times are between 7:00 a.m. – 9:00 a.m. or 12:00 noon – 2:00 p.m. Any times needed outside of these designated times will need to be arranged; send an email to lockshop@kent.edu. Authorized signatures are required to pick up the keys and identification is required.

Access to rooms is designated by the curator of the building or a designee. Designees must be identified by the curator through a work order or an email. High security spaces will require additional access approvals and will be considered on a case by case basis facilitated by the Lock Shop. Shared space access is also considered on a case by case basis.

Part time faculty and staff that use electronic key cards may need to have their cards reprogrammed each year. A quick email to the Lockshop will determine if the card needs to be taken back to the Lockshop for reprogramming or not.

Fees associated with new keys and cards can be found on the UFM website under Lock Shop.

Below is a checklist for requesting new hard keys and/or electronic key cards:

New Key Request Checklist

Hard Keys

* Create a Lock Shop work order through FAMIS or FlashTrack with the following information
* Identify individual receiving key(s) **and** provide Banner ID Number
* Identify designee, if other than curator or individual
* Identify room(s) with mechanical lock(s) individual is approved access to
* Submit work order

Electronic Key Cards:

* Create a Lock Shop work order through FAMIS or FlashTrack (using same information as above)
* Submit work order
* **Print off Electronic Lock Form A and fill out in its entirety** (Will be titled Electronic Lock Form once new website updated.) Form can be found at [www.kent.edu/ufm](http://www.kent.edu/ufm) > Lock Shop > Electronic Form A. Note: Incomplete forms will not be processed immediately.
* Submit Electronic Lock Form A to the Lock Shop via scanning and emailing to lockshop@kent.edu or fax to 330-672-7843 \*

\*At this time, FAMIS does not allow electronic submittal of the Electronic Lock Form with the work order.

Contact the Lock Shop by email at lockshop@kent.edu or by phone at 330-672-7846.

**Andrea Nunley – Director, Enterprise Application Services**

**Information Security is a Team Sport**

Information security is a top priority of the IS department. IS is responsible for providing and maintaining systems that are reliable, secure and accessible anytime, anywhere; thereby providing an information technology infrastructure that enhances productivity and enables global access. However, IS requires the help of all members of the Kent State community to protect sensitive data.

Information Technology (IT) security continues to be a top strategic issue facing institutions of higher education. The presence of critical information being available online makes securing and protecting information resources paramount. Kent State recognizes the need for vigilant security measures necessary to maintain the integrity of the electronic information produced by the Kent State community. Members of the Kent State community must be aware of any federally protected data and other sensitive data such as social security numbers that are stored on workstations and servers and we must take mandated steps to protect it.

* FERPA – Family Educational Rights and Privacy Act
* HIPAA – Health Insurance Portability and Accountability Act
* GLBA – Gramm-Leach-Bliley Act
* PCI DSS – Payment Card Industry Data Security Standards

Protection of sensitive data is achieved through encryption, firewalls, password protection, limiting access to privileged data, etc. Extra caution should be taken as breaches start with items such as email attachments and misplaced thumb drives.

Access to any of the Banner systems requires multiple levels of approval. A data confidentiality form needs completed by the employee requesting access, and approvals of access are required by the respective data steward and departmental security administrator. Access to the various systems should be granted to those individuals only if necessary as it relates to the scope of their daily job. Access should be based on need and not on convenience.

Any information on a shared drive should be scrutinized and sensitive data should be masked. As with access to Banner systems, access to shared drives should be granted as needed to perform daily activities.

IS role in protecting sensitive data:

* Review vendors that store KSU data offsite
* Mask sensitive data that is included but not necessary on reports and file extracts
* Conduct a sweep for sensitive data on departmental servers and fileshares
* Offer security awareness webinars

What can I do to protect sensitive data?

All employees need to be more conscientious of the documents that are being kept, saved, shared or sent. We all need to be aware of sensitive data that may be contained within documents as well as information that is being shared. When releasing information do not offer more information than is needed to complete the job and when requesting information don’t collect more information than is needed.

* Does your report or document contain sensitive data i.e. social security numbers?
* Is sensitive data in files that are sent to outside vendors or agencies?
* Is sensitive date being stored on your computer or fileshares?
* How are offsite vendors storing documents sent by KSU that may contain sensitive data?

If you have questions concerning files and data protection, contact IS.

* Ed Mahon - VP Information Services and CIO emahon@kent.edu
* Coleen Santee - Executive Director Information Services, Enterprise Support and Application Services csantee3@kent.edu
* Jason Wearley – Executive Director Information Services, IT Infrastructure Services and Support jwearley@kent.edu
* Brendan Walsh – IT Security Policy Manager, Security Access Management bmwalsh@kent.edu

**Lawrence Carter, KSU Foundation**

**KSU Hotel and Conference Center Asset Manager**

**KSU Hotel and Conference Center Named Preferred Hotel plus Stash Rewards**

Lawrence Carter was hired by the KSU Foundation as the asset manager and liaison between the KSU Hotel and Conference Center and Kent State University. Lawrence provided the group with a brief history of the development and opening of the KSU Hotel and Conference Center. The KSU Foundation financially supported the vision and serves as the primary lender allowing for earnings to flow back to the Foundation to be used for scholarships, grants, professorships and other university priorities.

Prior to 2014 Kent State University did not have a formal lodging contract with any hotel. An RFP (Request for Proposal) committee was established with the task of searching for and naming a hotel as the preferred hotel for university business. Four hotels submitted proposals and the KSU Hotel and Conference Center was selected based on 11 specifications and 29 requirements outlined in the RFP.

Kent State University requires the use of the KSU Hotel and Conference Center for business travel needs whenever they can provide suitable accommodations. IF the KSU Hotel and Conference Center is not available or cannot provide suitable accommodations, then the Sheraton Inn in Cuyahoga Falls and the Holiday Inn Express in Kent are the two alternates that have been chosen.

KSU’s relationship with the Hotel and Conference Center provides the university with many benefits:

* Designated KSU liaison – Lawrence Carter 330-672-7896 Lcarte19@kent.edu
* Designated hotel contact – Therese Kirkland (former KSU graduate) 330-968-6914 tkirkland@kentstatehotel.com
* Preferred rate of $109
* Group rates available
	+ Long term stay
	+ Large groups
* Customizable catering menu to work with department budget
* Understanding of the university billing requirements
* KSU Legal Counsel’s approved contract
* Direct billing
* Stash rewards
* Location, location, location – located at the foot of the esplanade

The KSU Hotel and Conference Center offers a Stash Rewards Program. This is a rewards program that includes over 200 hotels nationwide with 75 hotels on major college campuses. The program allows you to earn 5 points per $1 spent on sleeping rooms and special promotion offers on events and meetings. Points can be redeemed for free night stays but the stays must be university business related. Points can be tracked via email and can be redeemed on-line with no blackout dates.

The Stash Rewards program has been put in place with guidelines approved by the University Auditor’s office and Accounts Payable. Departments will be required to provide a department email address at the time of booking. Points redeemed will be redeemed towards university business also booked through that email address. Notifications will be sent periodically to the email addresses on file that have redeemed stash rewards points.

**Jo Ann Gustafson – Director, Internal Audit**

**Introduction of New IT Audit Manager**

The Office of Internal Audit exists to serve as an independent appraisal agency. As a service to management, the department examines and evaluates Kent State University’s activities with the goal of improving the efficiency and effectiveness of those activities. The office also serves as the liaison between the university and the university’s independent public accountant.

Jo Ann Gustafson introduced the newest member of the Internal Audit department, Annette Alboreo. Annette was hired as the university’s Information Technology (IT) Audit Manager, an area that was previously outsourced.

She comes to the university with 32 years of experience in the corporate world which includes six years as an IT Audit Lead, managing a team of auditors who focused on Information Technology audits and Sarbanes Oxley IT general control testing.  She spent 27 years in the IT department, with job assignments that included software development, IT technical trainer, developer support, security management, and project management.

As an IT auditor at KSU, Annette will be managing the Information Technology (IT) audit process to assist the university’s internal audit function by completing an information systems risk analysis, evaluating the effectiveness of technology controls, and reviewing systems that support business functions throughout the university. She will also assess compliance to security policy and controls for the University’s Banner ERP system.

**Anne Brown – Associate Vice President for Business and Administration Services**

**Administrative Policy for Credit Card Security**

Effective November 1, 2014 the university is implementing a university-wide compliance program regarding the security of credit card transactions. Kent State University is required to maintain compliance with Payment Card Industry Data Security Standards (PCI-DSS) which has been a topic of conversation for many months.

PCI-DSS applies to all transactions involving credit card information whether the transaction is processed by a university employee or by any other person or entity accepting credit card payments on behalf of Kent State University. The use of external third-party processing systems or utilization of internal university processing systems does not alter the processes needed for compliance purposes.

For the purpose of Payment Card Industry Data Security Standards (PCI-DSS) the following terms have been defined:

* Credit card – ANY branded card (including, but not limited to, American Express, Discover, MasterCard, and Visa) including debit cards and pre-paid cards. (As of the Oct. 8 forum, FlashCards are not included as a branded card but care must also be taken to safeguard the cardholder information.)
* Cardholder data – any personally identifiable information associated with a specific cardholder
* Merchant – departments and individuals who are authorized to accept credit cards as a form of payment for any type of university transaction

The Divisions of Business and Finance and Information Services are responsible for the policy implementation and coordination of the PCI-DSS mandate but ALL university offices and employees share the responsibility for continued adherence to this policy. There are significant fines administered if there is a breach or misrepresentation of the security of information.

**Minimum Requirements for PCI-DSS Compliance**

* Credit card transactions will be permitted ONLY using a secure PCI-DSS compliant university-approved electronic application or device. Departments wishing to accept credit cards will be responsible for the upfront fees to obtain the approved equipment or application as well as any ongoing fees. (The upfront fees will range from $500 - $1,000)
* Every employee involved in any aspect of credit card processing will be required to complete an online training module annually. Unique ID’s are required for each user; shared ID’s are not approved nor are they acceptable.
* Annual review is required; departments accepting credit cards will be required to complete a self-assessment questionnaire (SAQ) annually.
	+ The assessment is annually, but it will be an on-going process that must be monitored continuously
* NEVER accept or send cardholder data via fax or e-mail.
* NEVER use any type of imprint equipment to capture an image of a credit card.
* NEVER store cardholder data electronically
* Written cardholder data MUST be stored in a locked room or cabinet and must be redacted to only show the last 4 digits of the card number.
* Receipts must show only the last 4 digits of the card number.
	+ Please also note that this would include receipts showing payment using a university P-card where the entire card number is present.

If you become aware of a breach or a potential compromise of cardholder data it is important that you immediately notify the Bursar’s Office and the Office of Security and Access Management via e-mail to PCICompliance@kent.edu. This e-mail address will also be used for general questions regarding PCI-DSS so any urgent notifications should be marked as high importance (!).

Every department that currently accepts credit cards will receive a memo from Vice Presidents Gregg Floyd and Ed Mahon outlining the steps required to avoid interruption in your department’s ability to accept credit cards. The deadline for responding to the memo will be specified and failure to respond in the required timeframe will result in temporary suspension of your ability to process credit cards.

Departments will be provided guidelines and will be assisted with compliance, but they must actively participate in this process.

For full details regarding this policy “[Administrative policy regarding credit card security](http://www2.kent.edu/policyreg/policydetails.cfm?customel_datapageid_1976529=3861241)” refer to the Policy Register located on the General Counsel’s website, Policy number 7-01.2. (Due to the timing of website conversions, if the link is broken refer to the General Counsel’s main page, select Policy Register then the applicable policy number.)

**Contact information**

Preferred option: E-mail to PCICompliance@kent.edu

Direct contacts:

* Betsy Tierney, Bursar’s office ext. 2-0858
* Brendan Walsh, IT Security Policy Manager ext. 2-5566
* Anne Brown, AVP Business and Administration Services ext. 2-0984

**NEXT BAS FORUM**

**February 11, 2015**