

**BAS Forum Minutes**

**October 10, 2018 9:00 a.m. to 11:00 a.m.**

**Kent Student Center Governance Chambers**

**Mike Pfahl, Associate General Counsel**

**10 Tips Toward Better Contracting**

Mike reviewed 10 tips toward better contracting:

1. Know Your Partner.
2. Know how much you are paying, when you are paying, and why you are paying.
3. Know when the contract starts, ends, and whether you can terminate it early.
4. TGIC (Taxes, exempt; Governing law, Ohio; Indemnity, no; Confidentiality, to the extent permitted by law)
5. Protect our data. Contact IS if contract involving transmission, storage, creation of university data.
6. Check with Procurement. Maybe we already have a contract in place for this.
7. A contract doesn't have to look like a contract (offer or obligation + acceptance = contract)
8. Follow the policies. 3342-5-04.1, 3342-7-12, 3342-7-12.1
9. Sign with proper authority
10. Retain fully executed copy for Active + 6 years (PDF if fine).

Additionally Mike stressed the fact that all contracts need to be reviewed by legal counsel. Any agreement with an offer or obligation and an acceptance is a contract and it should be sent to [contracts@kent.edu](mailto:contracts@kent.edu) for review before it is signed.

The university has many approved contracts that have already been negotiated and approved by legal counsel. If you are looking for a specific service or vendor look to see if it/they are listed on the Procurement website as a preferred vendor. If you don’t see it/them check with Procurement to see if they can be added as a preferred supplier.

Be cautious of contracts where the vendor is asking for money upfront for a service; try to avoid deposits or negotiate the payment down.

Avoid auto-renewal of contracts. These become difficult to track (especially with office turnover) and grace periods often are overlooked extending contracts that are no longer needed.

Under the Ohio Revised Code (ORC) contracts involving travel cannot exceed limits established under university policy.

Only authorized personnel (those who have been delegated authority) can sign contracts on behalf of Kent State University. Per administrative policy 5-04.1:

*Contracting authority. For the purpose of this policy, "contracting authority" means university personnel who have been provided signing authority by express resolution of the Kent state university board of trustees, or university personnel that are provided authority through express written delegation from either the president of the university or the appropriate vice president, pursuant to the authority provided in rule 3342-5-04 of the Administrative Code.*

**Jeff Futo, KSU Police Services**

**Emergency Preparedness**

Jeff stressed with the forum members that it is our personal responsibility to keep ourselves safe and to know how to respond in the event of an emergency.

We must all be prepared. Knowing what to do in an emergency is key to getting through the emergency. Too often we don’t think about what we would or should do but we react and the reaction is not always in everyone’s best interest.

Do you know where the exits are in your building, not just the one you enter and exit through daily? Do you work with or know someone in your building that may be handicapped or require assistance in the event of an emergency? Have steps been made within your department(s) to prepare for an emergency and avoid unneeded panic due to the lack of preparation?

The university’s mass communication system broadcasts through desk phones, speaker systems in the building and FlashLine alerts. The alerts can be specific to certain areas and may or may not be broadcasted throughout the entire campus. Alerts could be weather related, shelter in place, lock down, evacuate, etc.

Each campus and each building on the Kent State campuses have emergency response plans. Ask your building curator for a copy pertaining to your building.

Departments should review emergency plans periodically with their staff. Do you review emergency shelters, exits, alarm locations, mass communication systems, etc. with new employees? Luckily emergencies are infrequent, but crisis mode is normally chaos so being prepared is the first step to successfully handling an emergency.

Another area to think about is business continuity following an emergency. What business processes may need to be handled remotely? Do the proper people have proper accesses outside of their offices? Are back up plans and processes documented? Again, emergencies are infrequent but plans need to be in place before the emergency arises.

Emergency Management information can be found on the Public Safety website: <https://www.kent.edu/publicsafety/emergency-management>

**Joseph Raftovich, Sr. Network Design Engineer - Telecommunications Services**

**Catherine Zapytowski, Sr. Business Manager, IS Administrative Support**

**PCR360 – New Billing System**

The old billing system, Pinnacle, used for telecomm billings has been replaced with a more robust system featuring much faster processes, Banner descriptions matching charge types, easier to read bills and easy to export files. Welcome PCR360.

If you reconcile your department’s index but do not have access to the telecom bills, email [pcrbilling@kent.edu](mailto:pcrbilling@kent.edu) to request access. Personnel listed as their department’s billing coordinator will receive an email every month notifying them that their monthly bill has been processed. The subject line on the email will be “Billing Transactions for xxxxx”. Within the email, there is a link to [pcr360.kent.edu](https://pcr360.kent.edu/), which is the site to view your billing transactions that appear on your monthly Banner reports. If you have a problem reading the bill, you can open a ticket at pcrbilling.kent.edu. System administrators can emulate you as the user so that they can see exactly what you are looking at.

The new system is better organized. It has more advanced features, more reporting options, and is cloud-based so it is accessible anywhere. You are sure to find the new system easier to use and significantly faster than Pinnacle. Expect to have a better all-around experience using this system.

Getting Started with PCR360

1. Access PCR360.kent.edu

2. Log in using your FlashLine username and password.

3. Hover over the Billing link under the PCR360 logo, then select View Bill.

Under Charge Accounts, you will find each of the account numbers (Banner index numbers) for which you are responsible.

Expand the account to view an itemized list of charges by Object Code (Banner expense account) and Service ID (phone number). This easily allows you to compare charges to their counterparts in Banner.

The billing contains subsets with object code summaries. Using the arrows to the left of the description, you can drill down into additional details.

The new PCR360 bill will show charges for all Information Services charges including audio visual rentals, server storage, faculty refresh machines, network and telecommunications charges, etc. Each outgoing phone call going off campus will have a fee assessed except for 1-800 numbers. Local calls are .08 each, and long distance calls are .08 per minute.

The Pinnacle billing system will be available until winter break, December 21, 2018. After this date, you will no longer have access to billings prior to the July 2018 service dates. Be sure to download any bills that you may need for your records.

When requesting assistance with or access to your information services billings, be sure to provide the telephone extension that you have a question about and the index number that the telephone line is being billed to.

**Brendan Walsh, Manager Security and Access Management**

**Cyber Security Awareness**

October is National Cyber Security Awareness Month (NCSAM) and Brendan reminded the BAS members of the various events happening around Kent State promoting awareness and protection of both university and personal business online. All of us need to do our part to ensure that our lives, both personal and business, are safe and secure.

University events throughout October

* Weekly activities – complete to be entered into a prize drawing
* Cyber Security Escape Room
* Visit information tables outside of the College of Business or on the 2nd floor of the student center
* Check FlashLine daily for a cyber security Tip of the Day
* Follow @KSUTechHelp for additional security advice
* Visit <http://SecureIT.kent.edu> for additional training materials and tips

Changing Your FlashLine Password and general password security

FlashLine does not currently prompt you to change your password but that does not mean you shouldn’t change your password(s) frequently. Changing your password in FlashLine changes most of your University passwords. However, in some cases additional steps may need to be taken regarding desktop encryption, Banner 9, Document Imaging, etc. Some other systems like development applications and BeWell Solutions have separate processes you have to go through to change passwords.

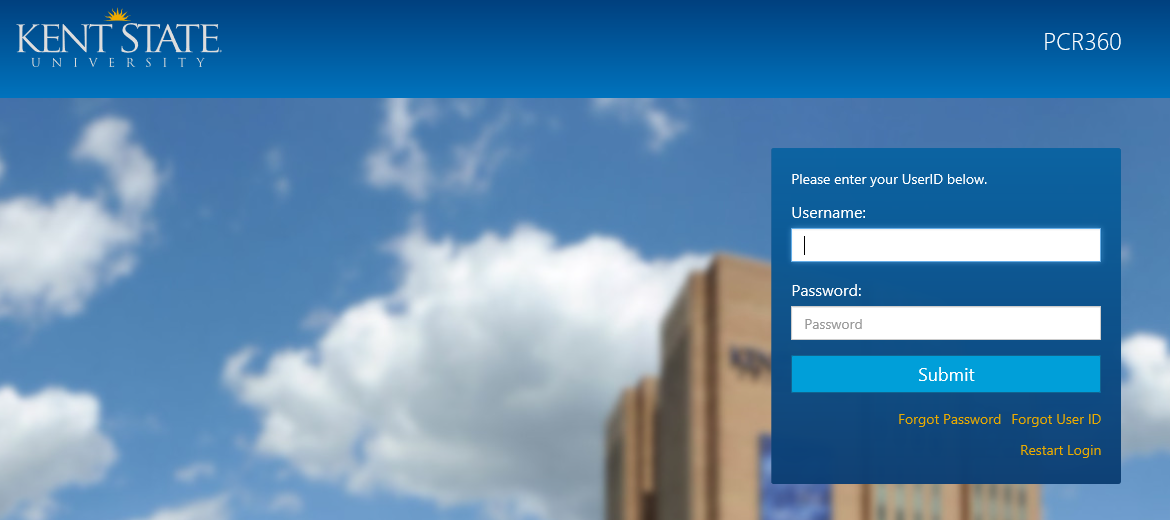
If you know your FlashLine password and want to change it, simply login to FlashLine, click on “Settings” in the left-hand navigation, and then click “Update Password” in the panel with your picture. If you do not know your current password, Visit [http://www.kent.edu](http://www.kent.edu/) and click on "FlashLine Login" or visit [http://flashline.kent.edu](http://flashline.kent.edu/). Click on “Forgot Your Password”, enter your FlashLine user name and click Next.

Answer Security Questions - Enter your answers to the security questions. Note: Your answers are not case-sensitive. After 3 unsuccessful attempts, your account will be locked. If this occurs, call the Helpdesk at 330-672-4357 (HELP) for assistance. Set New Password - Choose a new password and enter it twice for verification.

When you have entered your new password, click Submit. When you receive the “Success” dialogue box, click OK and you will be logged directly into FlashLine.

If you cannot remember the answers to your security questions, you can get assistance by calling the Helpdesk at 330-672-4357.  You may also request password assistance by coming in-person to the Library Walk-up Helpdesk (1st floor library) on the [Kent Campus or the assigned area for your campus](https://kent.teamdynamix.com/TDClient/KB/ArticleDet?ID=37973).

Always check the address when you see a page like the one below. Make sure it is located at kent.edu and is https encrypted. (You should see a green padlock in the toolbar.)



Passwords and password protection are areas that require due diligence.

Limit the number of times you reuse passwords across multiple sites. If one site is hacked, the hacker could gain access to other sites as well – any site where you reuse the same username and password. Ideally, use a separate password for each site. When establishing passwords you should rethink using the same methodology since one hacked password could lead to others. Longer and less complex passwords can be more secure than shorter very complex passwords and are often easier to remember. Hackers know the password tricks that we think are brilliant such as $ for letter S, + for letter T, 4 = for, beginning of password is a character or capital letter and ending is an exclamation point. In addition, family names and birthdates can be found on the internet so they are not safe options for passwords either. Our lives are on the internet so a lot of our personal information is not private.

Never share your passwords, even with the people you trust. Not only is it not safe, it is against university policy.

KeePass2 is a university-supported secure password vault. KeePass is an open source password manager where passwords can be stored. The database encrypts not only passwords but usernames also. KeePass is free and it is OSI certified. KeePass can be used for both business and personal password protection.

IT receives notifications of possible password breaches for kent.edu accounts. You can check your KSU and personal email accounts for breaches by going to <https://haveibeenpwned.com> This site includes the option to sign up for personal alerts as well.

Google Drives

Another area of security concern is when saving items to a Google Drive. Documents stored on a Google Drive are still bound by university retention requirements, university policies and compliance obligations. To determine the types of documents that can be placed on a Google Drive refer to KSU Google Terms of Service located at <https://www.kent.edu/sites/default/files/file/KSUGoogleTermsOfServiceUpdated-01-16-2018.pdf>. Compliance protected information, pcard information, banking information and data protected under HIPAA are a sample of documents that should not be placed on a Google Drive.

Distinguishing Sales Calls from Scams

The university is seeing a resurgence of telephone scams and fake invoices. Vendors that do business with the university should not be calling us asking for equipment ID’s, toner brands, model numbers etc. If you receive a phone call where the caller is asking for information, do not provide any information to them. Departments are responsible for purchasing items needed by their department and should be very leery when receiving phone calls relating to the purchase of business items and supplies.

Other phone scams could include calls from Microsoft support, Government Grant scams, IRS scam, Jury Duty scams etc. When the caller pushes for information, threatens to send you to collection, offers you a deal of a lifetime, indicates you qualify for grant money etc., raise the red flag and proceed with caution. Not all incoming phone calls like these are scams but to protect the university and/or your personal business, stop and request that the caller give you more information then tell them you will call them back. In most cases the caller will hang up; if they do not, verify phone numbers (research phone numbers through internet or mailing correspondence) and do your due diligence before proceeding.

Also along the same line, when signing off on invoices you need to verify that the invoices are valid. Be sure to review all invoices before sending them to Accounts Payable for payment; did your department order and receive the items listed on the invoice and is the invoice addressed to your department. Fake invoices are sent out in the hopes that someone is not paying attention and payment will be issued without asking questions. As stewards of university funds we need to protect our departments and the university by reviewing and verifying that the invoice is valid, accurate and only for a current amount due.

If you receive a phone call from a medical provider wanting you to make a payment over the phone or to set up a payment plan, again stop. Most billing statements provide you with options to pay by phone or on-line. You should initiate the phone call to set up payment arrangements and not be requested to provide banking information over the phone. Although the phone call may be valid, the disclosure of bank information should only be done using a trusted source.

Also remember that it is easy to spoof caller IDs and phone numbers. If you have caller ID you may see a phone number come up and it appears to be a valid number from a trusted source but the number may be compromised. If in doubt, ask questions and tell the caller that you will call them back. The number that the phone call is coming from may not be the actual number they are calling from. Be safe, be cautious and be diligent.

Saving Data Electronically

When saving data electronically you need to make sure that the data is safe and secure. Department shared drives are the best option. Shared drives are used to share all data types and the files are backed up frequently with several versions retained. Saving university data to a desktop drive is not recommended nor is it recommended to save data to thumb drives, a removable disk or to an external hard drive. It is to be noted that university policy for PCI compliance prohibits credit card information to be stored electronically in any fashion.

E-mail Security

E-mail is not a secure method for transferring data. Once e-mail leaves the KSU server it is no longer encrypted. Consider using Accellion to encrypt data and protect sensitive information (for more information contact IS).

Kent State will be deploying e-mail protection options very soon – including options to encrypt, mark messages confidential and restrict forwarding. Watch for upcoming information from IS regarding e-mail protection.

When sharing sensitive information with BeWell Solutions, be sure to use their BeWell portal. Sending information via e-mail is not encrypted once it leaves the KSU servers. The BeWell portal does encrypt data sent electronically.

Security is everyone’s responsibility. Whether it is personal business or university business we are all responsible for our own safety. Don’t let your identity be stolen, protect yourself and your personal data.

**Emily Hermon, Manager Accounts Payable**

**Gift Reporting Workflow**

The reporting of gifts has changed from a paper form to a workflow. Not only will the process reduce paperwork, it will allow the users to follow the process electronically.

One hour training sessions will be offered in November and December 2018 with the new workflow to begin in January 2019.

Watch for training opportunities via communication through the BAS ListServ and e-Inside.

**Mike Farina, Manager Financial Accounting**

**Banner 9 Upgrade**

Banner 9 Finance training was conducted in January and February 2018 and will be followed up with refresher courses next week. Banner 9 will replace Banner 8 over Fall break. The test environment for Banner 9 is available at <https://keys-ebudd.kent.edu/keys-test>. Everyone is encouraged to utilize the test environment for practicing in Banner. The test environment (use either eMock or eQA) will allow you to get used to the new format of Banner 9 while not having to worry about the data that you are entering.

If you are unable to access the test environment, contact either Melissa Berry or Sherri Stevens for assistance.

The test environment is not updated regularly so FY19 data is limited to information since the last update and test transactions performed in FY19.

Finance training guides can be bound on the BAS website at [www.kent.edu/bas](http://www.kent.edu/bas) under Banner Tips & Quick Guides.

**NEXT BAS FORUM**

**WEDNESDAY**

**FEBRUARY 13, 2019**

**SCHWARTZ CENTER AUDITORIUM**