University of Idaho
A LEGACY OF LEADING

Council of the University of Idaho Business Officers
Summary Notes
March 12, 2015

Purchasing Card Compliance and Consequences- Kent Nelson, General Counsel

Kent was unable to attend. He will appear on April's agenda. This presentation will be at FIG and all are encouraged to attend.

PCI Compliance Overview- Kim Salisbury, Controller's Office

Companies that supply credit cards formed a security council to abide by standards to protect individuals' card information. DSS 3.0n enforced by companies themselves, not government or counsel. Our credit card processor is Elavon. Elavon requires us to be PCI compliant at all locations, market place, athletics, student accounts, etc. Internal Audit completed an audit last year to determine where we are in terms of compliance. Findings included areas of improvement. We are currently charged $35 per month per merchant. Any place that takes a card swipe is an individual merchant.

See handout for more information to report back to Elavon, we are required to self-assess.

Overall the UI policy will need to be updated to include incident response from ITS and training.

The email sent out in February included who would need to take training. The last page of the handout includes who is required to take the training- essentially anyone who takes a credit card payment.

Service Procurement Agreements v. "Service Center" Agreements- Julia McIlroy, Purchasing

There is clarification needed regarding what constitutes a service center agreement and what requires a procurement agreement from Contracts and Purchasing.

Simply-

Service Procurement Agreements- the University of Idaho is receiving service and issuing payment; Contracts and Purchasing handles this.

"Service Center" Agreements- the University of Idaho is giving a service and receiving payment; OSP handles this to oversee any research conducted. This does not necessarily mean it is a grant but they are required to review and sign the agreements to verify.

Sodexo Catering, Internal Meal Compliance- Linda Keeney, Accounts Payable/Brad White, Internal Audit

An audit on was completed on paying meals on pcards. Policy 70.22 in the APM outlines the requirements for internal meals. There have been questions regarding the documentation needed for

internal meals. The policy states there must be more than five people, there should be someone outside of the organization in attendance, a list of attendees provided, a published agenda, and an entertainment waiver completed.

Other questions have been because of Sodexo and the documentation needed. These charges are processed through an IDG by Auxiliaries with what limited information given to them. There is a form that departments fill out with basic information. It is the department's responsibility to obtain the entertainment forms. Sodexo is no different than any other vendor. Requirements for catering remain the same.

This topic will be revisited to update the policy and provide more clarification.

Asset Accounting Updates- Brenda Marsh, Asset Accounting

See attached handouts for information.

Department Updates

OSP- The final candidate for the open Director position will be March 23, at 11:00 a.m. in Morrill Hall.

No other reports.

About Us

Text size −|+ · Share ▾ · Print 🖶 · 🐦 in

Overview

Organizational Structure

PCI SSC Committees

Board of Advisors

PCI SSC Executive Staff

Jobs at PCI

Contact Us

About Us

About the PCI Security Standards Council

The PCI Security Standards Council is an open global forum, launched in 2006, that is responsible for the development, management, education, and awareness of the PCI Security Standards, including the **Data Security Standard (PCI DSS)**, **Payment Application Data Security Standard (PA-DSS)**, and **PIN Transaction Security (PTS)** requirements.

The Council's five founding global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. -- have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs. Each founding member also recognizes the QSAs, PA-QSAs and ASVs certified by the PCI Security Standards Council.

All five payment brands, along with Strategic Members, share equally in the Council's governance, have equal input into the PCI Security Standards Council and share responsibility for carrying out the work of the organization. Other industry stakeholders are encouraged to join the Council as Strategic or Affiliate members and Participating Organizations to review proposed additions or modifications to the standards.

On this website you'll find useful information about the PCI Security Standards Council, the PCI DSS requirements for merchants, vendors and security consulting companies, and the Council's certification and merchant support services, all created to mitigate data breaches and prevent payment cardholder data fraud.

Note that enforcement of compliance with the PCI DSS and determination of any non-compliance penalties are carried out by the individual payment brands and not by the Council. Any questions in those areas should be directed to the payment brands.

Getting Started with PCI Data Security Standard

Data security for merchants and payment card processors is the vital byproduct of applying the information security best practices found in the Payment Card Industry Data Security Standard (PCI DSS). The standard includes 12 requirements for any business that stores, processes or transmits payment cardholder data. These requirements specify the framework for a secure payments environment, but for purposes of PCI DSS compliance, their essence is three steps: Assess, Remediate and Report.

Assess is the process of taking an inventory of your IT assets and business processes for payment card processing, and analyzing them for vulnerabilities that could expose cardholder data. **Remediate** is the process of fixing those vulnerabilities. **Report** entails the compilation of records required by PCI DSS to validate remediation, and submission of compliance reports to the acquiring bank and card payment brands you do business with. Doing these three steps is an ongoing process for *continuous* compliance with the PCI DSS requirements. These steps also enable vigilant assurance of cardholder data safety.

PCI DSS COMPLIANCE IS A CONTINUOUS PROCESS

ASSESS

REPORT

REMEDIATE
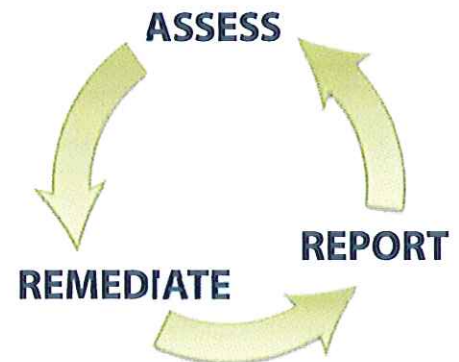
"PCI DSS represents the best available framework to guide better protection of cardholder data. It also presents an opportunity to leverage cardholder data security achieved through PCI DSS compliance for better protection of other sensitive business data – and to address compliance with other standards and regulations."

AberdeenGroup
IT Industry Analyst

PCI Data Security Standard Requirements

PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process, and/or transmit cardholder data. It presents common sense steps that mirror best security practices.

Goals	PCI DSS Requirements – Validated by Self or Outside Assessment
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Step 1 – Assess

The primary goal of assessment is to identify all technology and process vulnerabilities posing a risk to the security of cardholder data that is transmitted, processed or stored by your business. Study the PCI DSS on our web site (www.pcisecuritystandards.org) for detailed requirements. It describes IT infrastructure and processes that access the payment card infrastructure. Determine how cardholder data flows from beginning to end of the transaction process – including PCs and laptops which access critical systems, storage mechanisms for paper receipts, etc. Check the versions of personal identification number (PIN) entry terminals and software applications used for payment card transactions and processing to ensure they have passed PCI compliance validation.

Note: your liability for PCI DSS compliance also extends to third parties involved with your process flow, so you must also confirm that they are compliant. Comprehensive assessment is a vital part of understanding what elements may be vulnerable to security exploits and where to direct remediation.

Self-Assessment Questionnaire (SAQ). The SAQ is a validation tool for eligible merchants and service providers who self-evaluate their PCI DSS compliance and who are not required to submit a Report on Compliance (ROC). A number of SAQs are available for different environments; see table below and our web site for details:

SAQ	Description
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. *This would never apply to face-to-face merchants.*
B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage
C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage
C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage
D	All other merchants not included in descriptions for SAQ types A through C above, and **all service providers** defined by a payment card brand as eligible to complete an SAQ

Qualified Assessors. The Council provides programs for two kinds of independent experts to help with your PCI assessment: Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). QSAs have trained personnel and processes to assess and prove compliance with PCI DSS. ASVs provide commercial software tools and analysis services for performing external vulnerability scans for your systems. The PCI SSC also provides educational resources for merchants and service providers, including training for Internal Security Assessors (ISAs). Visit our Web site at www. pcisecuritystandards.org for details and links to qualified assessors and training resources.

Step 2 – Remediate

Remediation is the process of fixing vulnerabilities – including technical flaws in software code or unsafe practices in how an organization processes or stores cardholder data. Steps include:

- Scanning your network with software tools that analyze infrastructure and spot known vulnerabilities
- Review and remediation of vulnerabilities found in on-site assessment (if applicable) or through the self-assessment process
- Classifying and ranking the vulnerabilities to help prioritize the order of remediation
- Applying patches, fixes, workarounds, and changes to unsafe processes and workflow
- Re-scanning to verify that remediation actually occurred

Step 3 – Report

Regular reports are required for PCI DSS compliance; these are submitted to the acquiring bank and payment card brands that you do business with. PCI SSC is not responsible for enforcing PCI DSS compliance. All merchants, service providers and processors may be required to submit quarterly scan reports, which must be performed by a PCI SSC approved ASV. Businesses with larger transaction volumes have an annual on-site assessment completed by a PCI SSC approved QSA and submit the findings to each acquirer. Businesses with smaller transaction volumes may be required to submit an annual Attestation within the Self-Assessment Questionnaire. For more details on validation and reporting requirements, speak with your acquirer or payment card brand. Please also visit our web site at: www.pcisecuritystandards.org.

Employee training is one of the requirements of PCI-DSS. The University of Idaho is going to use a training series from the SANS Institute, entitled Securing the Human, to educate all personnel about the importance of securing credit card information. Training will be mandatory upon start of employment and yearly thereafter for any employee who:

- Has access to credit card data
- Receives credit card information in any manner, such as over the phone, in person, or online
- Processes credit card transactions
- Transports credit card information
- Has access to Marketplace Stores or other online application containing credit card information

The current plan is to have this training series available to employees starting March 31, 2015. Please complete the training as soon as possible, as there is a deadline of June 30, 2015.

More specific information will be sent out to employees who are signed up for the training as we near the end of March.

Asset Accounting Update
CUIBO – 3/11/2015

Please pass this information along to anyone in your department who might be interested.*

1) <u>Upcoming Property Management Training:</u>
   a) Training will be held March 18th from 1:30 – 4:30 in the Commons Whitewater room. It will be presented by Joe Groves and will be available via video conferencing.
   b) Anyone who is interested can sign up for the training (titled *Asset Management & Inventory Training*) via NetLearning at www.uidaho.edu/netlearninglogin.
   c) This is the first official training session we have offered in the last couple of years, and there have been many changes and improvements in our processes, so anyone who has an interest in or responsibility for equipment asset management is highly encouraged to attend.
   d) The training and Q&A session will be videotaped in its entirety to accommodate those who aren't able to attend due to spring break or other conflicts. We intend to use this video for ongoing training purposes as well, until such time as another formal training session is warranted or requested.

2) <u>New Asset Change Request Process:</u>
   a) Until recently, requests for changes and updates to equipment asset records had to be done via phone calls and e-mails, then the same information was manually entered by our office in Banner, resulting in many hours spent on back and forth communications and duplicated efforts (e.g. multiple people typing the same serial number several times, playing phone tag, time spent by many combing through the dreaded "reply all" e-mails, etc.).
   b) In the spirit of continuous improvement, our office worked with Kim Salisbury (Business Processes), Creg Empey (ITS Enterprise Applications), and several "testers" to develop a new application that allows most equipment asset changes to be requested via VandalWeb.
   c) Types of asset changes that can be requested in VandalWeb include:
      i) Asset information changes, including descriptions, serial numbers, make/model, and manufacturer;
      ii) Usage status (e.g. active, idle, etc.) and condition changes;
      iii) Location or custodian changes;
      iv) Transfers to another department;
      v) Disposals via transfers to Surplus; and

vi) Other disposals (e.g. trade-ins, transfers to other universities/agencies, etc.)

d) There is an approval queue similar to Banner approvals, which includes approvals by Surplus and OSP where applicable.

e) For most changes, once the change is approved, the asset record in Banner is also automatically updated, which further reduces time spent by our office on manual processing and results in fewer manual input errors. However, disposals will always be manually entered by our office to ensure assets are not disposed of accidentally, and grant funded equipment transfers will also continue to be entered manually to ensure compliance with grant requirements.

f) Several slides from the upcoming training session are included here, but we will go through this in much more detail during the training.
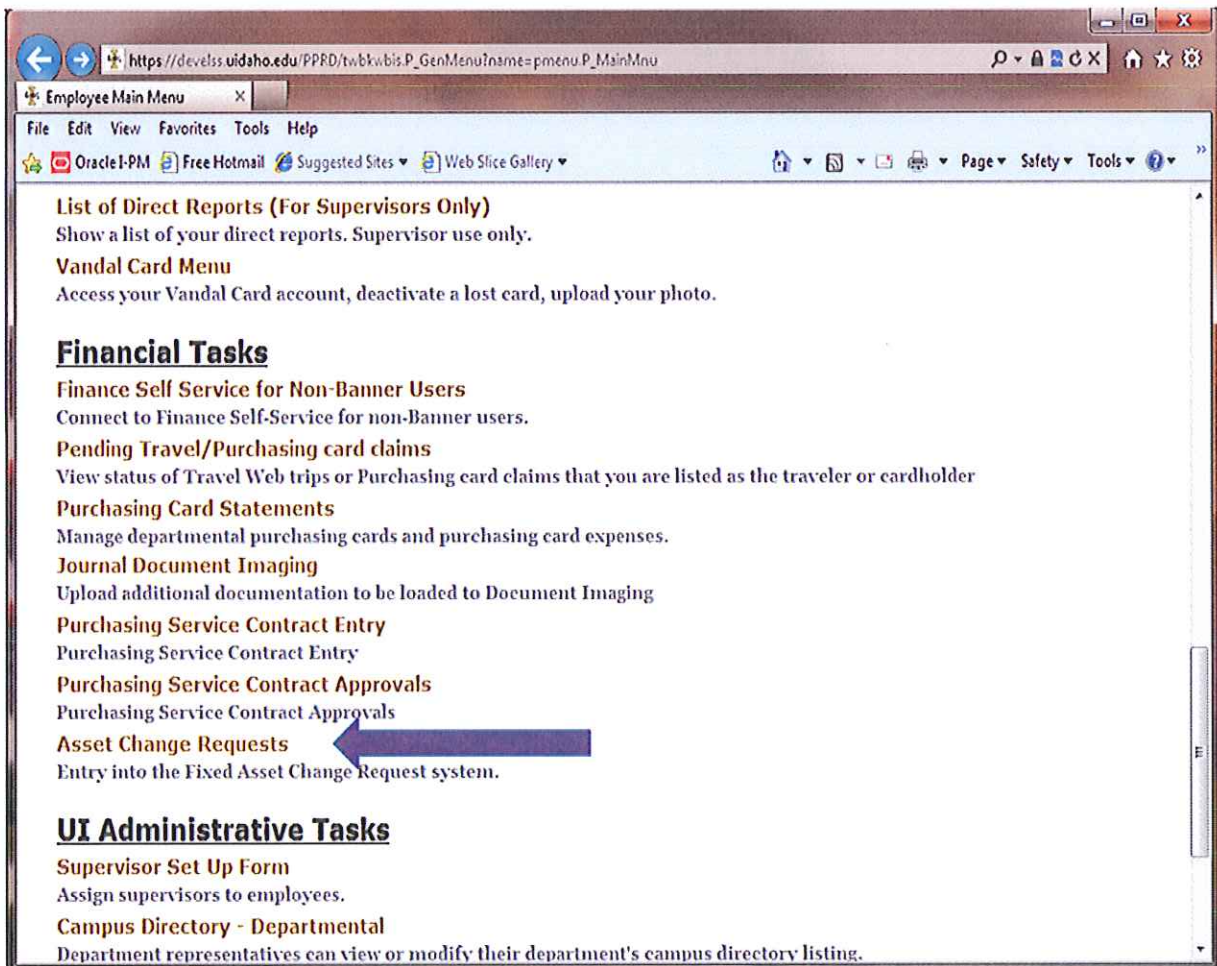
Location and Custodian Change Request

File Edit View History Bookmarks Tools Help

UI Asset Accounting x +

https://vandalweb.uidaho.edu/PROD/ui_fin_asset_change_user.process_approval   Search

University of Idaho

ADMINISTRATION | ASSET CHANGE REQUESTS | VANDALWEB | LOGOUT

Messages

Request approved.

New Request

Permanent Tag # 196968   [Go]

Requests Pending Your Approval

Permanent Tag #	Originator	State	Last Activity
402845	Groves, Joseph E.	Pending Surplus Approval	05-Dec-2014

Requests You Have Submitted

Permanent Tag #	Originator	State	Last Activity
402845	Groves, Joseph E.	Pending Surplus Approval	05-Dec-2014
402603	Groves, Joseph E.	Completed	04-Dec-2014
121484	Groves, Joseph E.	Completed	05-Dec-2014

DIRECTIONS AND MAPS | CONTACT US | POLICIES AND COPYRIGHTS | ACCESSIBILITY | DIVERSITY | GIVE TO THE UNIVERSITY OF IDAHO

Location and Custodian Change Request

File Edit View History Bookmarks Tools Help

UI Asset Accounting x +

https://vandalweb.uidaho.edu/PROD/ui_fin_asset_change_user.start_new_ptag   Search

University of Idaho

ADMINISTRATION | ASSET CHANGE REQUESTS | VANDALWEB | LOGOUT

Asset Identifying Information

Permanent Tag #196968   Origination Tag #T00094625   System Status: Non Banner Procured Assets   Cap Ind: N   Book Value: $2040
Description: COMPUTER

Current Descriptive Information

Asset Description	COMPUTER
Make	SAGER
Model	NP8268-S (CLEVO P150SM-A)
Manufacturer	SAGER
Serial Number/VIN	

Current Status Information

User Status	Active
Condition	Excellent
Responsible Orgn	BJX017 Plant, Soil & Entomological Science
Location	AY242 Ag Science Bldg-Room 242
Custodian ID	V00515153 Thompson, Nicole M.
Equip Mgr ID	

[Update Descriptive Information]   [Update Status Information/Transfer Asset]

DIRECTIONS AND MAPS | CONTACT US | POLICIES AND COPYRIGHTS | ACCESSIBILITY | DIVERSITY | GIVE THE UNIVERSITY OF IDAHO

3

Location and Custodian Change Request

File Edit View History Bookmarks Tools Help

UI Asset Accounting

https://vandalweb.uidaho.edu/PROD/ui_fin_asset_change_user.update_status_info   Search

University of Idaho

ADMINISTRATION | ASSET CHANGE REQUESTS | VANDALWEB | LOGOUT

Asset Identifying Information

Permanent Tag #196968   Origination Tag #T00094625   System Status: Non Banner Procured Assets   Cap Ind: N   Book Value: $2040
Description: COMPUTER

Current Status Information		New Status Information		
User Status	Active	User Status	Active	
Condition	Excellent	Condition	Excellent	
Responsible Orgn	BJX017 Plant, Soil & Entomological Science	Responsible Orgn	BJX017	Plant, Soil & Entomological Science
Location	AY242 Ag Science Bldg-Room 242	Location	AY317	Ag Science Bldg-Room 317
Custodian ID	V00515153 Thompson, Nicole M.	Custodian ID	V00087132	Prather, Timothy S.
Equip Mgr ID		Equip Mgr ID		
		Disposal Requested?	No	
		Reason for Change	Change Location/Custodian ID.	

[Discard Request] [Save and Exit]   [Finish and Submit]

DIRECTIONS AND MAPS | CONTACT US | POLICIES AND COPYRIGHTS | ACCESSIBILITY | DIVERSITY | GIVE TO THE UNIVERSITY OF IDAHO

Location and Custodian Change Request

File Edit View History Bookmarks Tools Help

UI Asset Accounting

https://vandalweb.uidaho.edu/PROD/ui_fin_asset_change_user.view_request?id=103   Search

University of Idaho

ADMINISTRATION | ASSET CHANGE REQUESTS | VANDALWEB | LOGOUT

Asset Identifying Information

Permanent Tag #196968   Origination Tag #T00094625   System Status: Non Banner Procured Assets   Cap Ind: N   Book Value: $2040
Description: COMPUTER

Field	Current Information	New Information
Responsible Locn	AY242 Ag Science Bldg-Room 242	AY317 Ag Science Bldg-Room 317
Custodian ID	V00515153 Thompson, Nicole M.	V00087132 Prather, Timothy S.
Reason for Change	Change Location/Custodian ID.	

Approve this Request:
◉ Approve
○ Disapprove
Reason for Disapproval:

[Submit Query]

Approval from   Approved by   Date
Originator   V00011059 Groves, Joseph E. 05-DEC-14

DIRECTIONS AND MAPS | CONTACT US | POLICIES AND COPYRIGHTS | ACCESSIBILITY | DIVERSITY | GIVE TO THE UNIVERSITY OF IDAHO

Location and Custodian Change Request

Oracle Fusion Middleware Forms Services: Open > FFAMAST

File Edit Options Block Item Record Query Tools Help

Fixed Asset Master Maintenance FFAMAST 8.7.0.2 (* PROD *)

Asset Tag: 196968 ▼   Action: Permanent Tag - Update Asset ▼

Procurement Information FFAMAST 8.7.0.2 (* PROD *)

Origination Tag: T00094625   Permanent Tag: 196968   COMPUTER

Vendor:
Purchase Order: Purchase Item:
Receiver: Receiver Date: 24-JUN-2014
Invoice: Invoice Date: Submission Number:
Invoice Item: Cancel Date:
Credit Memo: Installments: Recurring:

Other Source Data

Document: Type: Sequence: Document Tag Date: Submission Number:

Transfer Data

Date: 05-DEC-2014
COA: 9 ▼ University of Idaho COA
Organization: BJX017 ▼ Plant, Soil & Entomological Science
Location: AY317 ▼ Ag Science Bldg-Room 317
Grant: ▼
Custodian ID: V00087132 ▼ Prather, Timothy S.
Equipment Manager: ▼

Enter responsible COA
Record: 1/1   <OSC>

3) <u>New Argos Inventory Reports Process:</u>
   a) The annual equipment inventory process used to be kicked off each August by our office downloading information for and preparing approximately 180 Excel files to be sent to the property administrators who were in charge of keeping track of the equipment. They would then verify the equipment and send back the completed inventories. This used to be done manually with hardcopies, which was obviously very time consuming and an inefficient use of other campus resources such as Campus Mail. We converted this to an electronic process via e-mail over the last two years, which was much more efficient, but could still be improved upon.
   b) In the spirit of continuous improvement, our office worked with Kim Salisbury (Business Processes), Mike Beery (ITS Enterprise Applications), and several "testers" to develop a new report in Argos that allows property administrators to run and download their own inventory reports and then sort and arrange them in the format that is most useful to them.
   c) Once the administrators have the reports downloaded and saved exactly as they like them, they can complete their inventories and then e-mail them back to our office along with the signed certification. They will also be able to enter most of their changes through the new Asset Change Request process described previously.

d) Several slides from the upcoming training session are included here, but we will go through this in much more detail during the training.

Enter department number and date, then click on the green gear

Department number: M003

Inventory obtained before: 02/19/2015

You can run this by responsible orgn or by midlevel dept number. Example: If I run the report with the midlevel dept number, it will return ALL responsible orgns assigned to CNR's inventory.

Save the report in .csv format first, then you can Save As in Excel format. From there, you can sort and arrange in the format most useful to you.

4) Equipment and Other Leases:

   a) The University's leases have been a little troublesome to track, analyze and account for effectively, so we are now in the process of trying to get our arms around everything that is lease related by centralizing all lease analysis and accounting within Asset Accounting.

   b) Below is a slide that will be shown during the training; however, leases are directly related to the accounting side of the office, so all lease related information (including long-term rentals) should be sent to my attention at brendam@uidaho.edu.

   c) We are working on developing and documenting procedures for lease related activities and accounting, but for the time being, please ask anyone and everyone who has anything to do with leased equipment or other kinds of leases to forward the information on what is being leased. I will follow up with them for any additional information I need.

Leased Equipment

- Asset Accounting is now the central location for lease analysis and accounting.

- All leases of equipment that would otherwise have a purchase price of $5,000 or more need to be funneled through our office so they can be properly analyzed to determine if they are capital or operating leases.

- The assumption cannot be made that a lease is automatically an operating lease just because it is a copier or similar equipment – there are very specific accounting rules that need to be applied before that determination can be made.

- We are in the process of looking at lease-related procedures and E-codes and will update the information when it is completed.

- For now, please send all lease information (contracts, lease schedules, etc.) to us so we can account for them properly in our financial statements.

5) Equipment Verifications:

   a) Verifications are now being done on an ongoing basis year round, so all departments should be expecting to hear from us at some point if they haven't already.

   b) We plan to make return visits more often to departments with more problematic verifications and inventories to assist them however we can in an effort to get them into better compliance with the University's asset management policies. We have already seen improvements from our efforts, so we are looking forward to continuing to improve in this area.