Welcome to the very first newsletter from the Financial and Operational Audit office. We are the University's internal auditors. The purpose of this newsletter is to inform the NKU community about audit related issues and concerns. We all share in the responsibility of establishing appropriate controls and monitoring their effectiveness. It is our goal that this and subsequent issues of Audit Alert assist you with that process.

The FOA office is a department within the Division of Administration and Finance. Our office is located in 504 Lucas Administrative Center. Each Audit Alert issue will address topics such as Internal Controls, Fraud, Management Responsibilities and Security.

Please feel free to forward comments, questions or suggestions:
Larry Meyer, director
phone 572-6117 e-mail meyerl3@nku.edu
Meghna Singhvi, staff auditor
phone 572-1345 e-mail singhvim@nku.edu

Occupational Fraud: What Is It?

Fraud can be defined as using one’s occupation for personal enrichment through the deliberate misuse or misappropriation of an employer’s resources or assets. Occupational fraud can be as simple as stealing office supplies or as complex as manipulation of the financial statements of a multi-national corporation.

According to the Association of Fraud Examiners occupational fraud has four key elements in common:

- Is clandestine
- Violates perpetrator’s fiduciary duties to the organization
- Committed for the purpose of direct or indirect financial benefit to the perpetrator; and
- Costs the company assets, revenue or reserves.

The Association of Fraud Examiners estimates that organizations can lose up to 5% of their revenue due to occupational fraud.

Common Types of Fraud Occurring in Higher Education

- Misuse of University Procurement Card
- Diverting/Skimming payments or deposits
- Falsifying records such as timesheets or purchasing documents
- Using university assets or technology for personal use

Tips to Prevent or Reduce Occupational Fraud

1. Design procedures to ensure adequate oversight and segregation of duties. One employee should not be responsible for initiating, approving and reconciling a financial transaction.
2. Supervisors should monitor the activity that occurs in their departments. Review documents thoroughly
before you approve them. If you don’t understand a transaction—ask questions.

3. Supervisors should also review their SAP accounts monthly (preferably more often) to ensure that all transactions are appropriate. Investigate any transactions you didn’t approve or don’t understand.

4. Supervisors can and should review all procurement card transactions that are made in their department. Contact the Procurement Services department for more information (572-5265).

5. All payments should be deposited within 24 hours of being received. Supervisors should review their SAP records to verify that transmittal deposits were recorded. Again, segregation of duties should be established to ensure that one employee is not permitted to receive, record and deposit payments. One way to achieve proper segregation is for one employee to log in all payments and another employee prepare the deposit. Supervisors should compare the log to the deposits to ensure they are in agreement.

6. Fraudulent activity involving upper management typically involves override of internal controls because they have the ability and the access. Reducing this ability and access reduces opportunity.

7. Before you hire a new employee make sure that you learn as much about the candidate as possible, check references, etc. Contact Human Resources for more information (572-5200).

8. Let employees know that honest and ethical behavior is expected. Set the tone at the top of your organization.

9. Establish lines of communication so employees feel comfortable reporting fraud or wrongdoing to their supervisor. Most fraud is discovered from tips received from other employees.

10. It’s more efficient and effective to put preventative controls in place to reduce the chance of fraud before it occurs than it is to use detective measures to identify the crime after it has occurred.

It is important to remember that fraud detection and prevention is the responsibility of every employee. If you have concerns bring them to the attention of your supervisor or the Financial and Operational Audit (572-6117).

---

**COMPUTER SECURITY TIPS**

**Backing-up files is important** – Hard drives can just stop working, files sometimes become corrupted or you might accidentally delete a much needed file. Back up your files regularly and store the backups in a dry and safe place.

**Passwords** – Never share your password no matter how much you trust that person. Use a password that contains special characters such as #, * or %. This increases the time it takes to crack a password. Change your passwords frequently, at least every 90 days or whenever you feel it has been compromised. And don’t write down your password and put it next to your computer!

**Install antivirus software** – Install the most current version of the antivirus program on your computer and establish a schedule for scans. Also make sure you configure your computer to receive automatic updates. Scans should be completed at least weekly.

**Install security updates** – Microsoft frequently sends out updates to their Windows Operating Systems. Make sure you keep your computer updated for important security patches.

**Be cautious of e-mails from unknown sources** – Don’t open e-mails from senders that you don’t know. And don’t respond to request for personal information like bank account numbers, credit card information and social security numbers.

**Laptop, flash drives** – When using laptops, flash drives, palm pilots or other hardware that can be easily lost or stolen make sure it is password protected. Sensitive data should always be encrypted or not stored on this type of hardware.