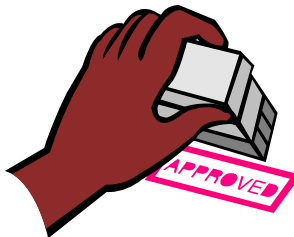


Appropriate Approvals

To assure proper segregation of duties, employees should not approve their own transactions or documents. These transactions or documents include, but are not limited to: *Check Requests*, *Employee Personnel Action Forms (EPAFs)*, and *Travel Authorizations*. An independent review helps to protect the employee from any real or perceived conflicts of interest or any question about the appropriateness of the transaction. The approver should be someone at least one supervisory level above the requester or recipient of funds.



For information relating to approvals of *EPAFs* and proper proxy assignments, please see University Policy 519 *Approval Authorization for Personnel Actions* (effective August 2007) <http://www.usu.edu/hr/policies/section500/519.pdf>

INSIDE THIS ISSUE

- 1 Appropriate Approvals
- 1 Expense Account Codes
- 2 Commuting vs. Travel Expenses
- 2 Spider Tool to Check Computer Data

Expense Account Codes

The Controller's Office has established hundreds of detailed expense account codes in Banner. Account codes should provide specific information about the nature of the expense. Proper classification produces more accurate financial reports.

Account codes like 715800 "Other Current Expense" or 715850 "PCard Other Current Expense" do not provide specific, meaningful information. Use of these generic, non-specific codes should be the exception rather than the rule.

Purchasing Card transactions are imported into Banner from U.S. Bank data. Depending upon the vendor, the default account code recorded in Banner is often 715850 "PCard Other Current Expense." This expense account code does not tell management anything about the true nature of the expense. These transactions should be re-classified to reflect the specific nature of the expenditures, e.g., freight and postage, receptions and guests, office supplies, etc.

Check Request Forms and *Requisitions* should also be completed with the most descriptive account code.

Also, revenue should be properly reported using a revenue account code, not as a negative expense.

The Controller's Office plans to post all current account codes on their website in April: <http://www.usu.edu/controller> If you are unsure about the appropriate account code to use, contact your accountant.

Commuting vs. Travel Expenses

What distinguishes “commuting” which is a personal expense from “travel” which is a business expense paid or reimbursed by the University?

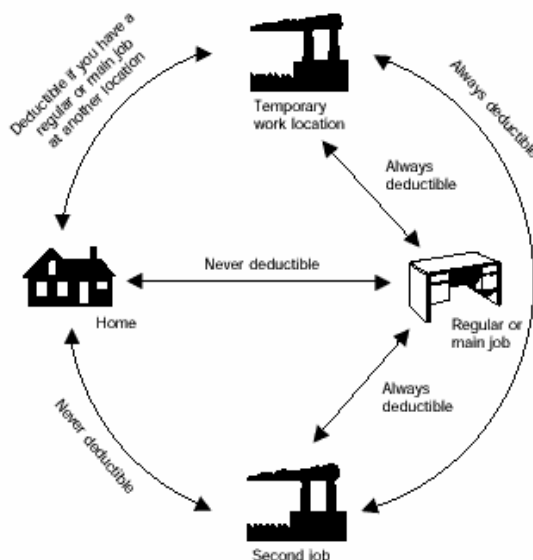
In general, the following rules apply when determining whether transportation and lodging expenses are business or personal expenses:

U.S. Code 26, Section 162 defines deductible (or tax exempt if reimbursed) travel as business expenses “while away* from home** in the pursuit of a trade or business.”

* Per Revenue Ruling 94-47, “away from home” is a temporary work location outside the metropolitan area where the employee normally works.

** Revenue Ruling 73-529 defines a taxpayer’s home as his regular or primary place of business or if he has no regular or principal place of business...then at his regular place of abode.”

Expenses listed as deductible in the IRS illustration below are proper business expenses which are excludable from taxable wages if reimbursed by the University:



Spider Tool to Check Computer Data

Prior to using “A” numbers as employee or student identifiers, departments may have used social security numbers. Human Resources and Payroll retain this data in a secure manner. But no other department should save sensitive employee or student data either in hard copy or electronic files. This sensitive data is vulnerable to fraud and misuse.

Cornell University has developed a FREE software program (Spider) which searches hard drives for sensitive data like social security numbers, credit card numbers, etc. The search does result in some false positives — meaning no sensitive data is contained in the file. However, this software is a helpful tool to identify files on your hard drive which may contain sensitive data. Download here:

<http://www.cit.cornell.edu/security/tools/>

After the “Spider” is run, the log file will list the paths of suspect files. Confirm the existence of sensitive data by viewing the file. If the file contains sensitive data, replace the data, i.e., A# for SSN, encrypt or erase the file. “Delete” is not the same as “erase”. To read more about the difference and download FREE erase software: <http://www.heidi.ie/eraser/>

For further information or assistance, please contact information technology (IT): <http://it.usu.edu/hm/contact>

“Audit News”

A Publication of Internal Audit Services
 Utah State University
 Old Main Hill, Room 63
 435-797-1084 * **Hotline: 435-755-7118**
<http://www.usu.edu/ias/>



INTERNAL AUDIT SERVICES
 INTEGRITY · ACCOUNTABILITY · SECURITY