**Travel Changes Effective February 1, 2017**

1. Meals will now be reimbursed according to what the traveler actually spent up to the amount of per diem rate for each meal.  Travelers will now need to **save their meal receipts** and turn them in to their travel specialist when they submit their travel claim(s).
2. Travelers may receive meals for same day travel.  In order to do this the traveler must be at least 50 miles from their duty post **and** in travel status for at least 6 hours.  Again, travelers will need to save their receipts for meals.  Please be aware that **same day meals** are considered taxable income and will be taxed.
3. If a lodging establishment offers a continental breakfast, it will now be considered a viable meal and travelers will not be able to claim breakfast for that day.    In the past, if the meal did not include protein, travelers could purchase their meal elsewhere and be reimbursed.  That is no longer the case.
4. If a travel specialist has paid for the travelers expenses with a university purchasing card and the traveler will have no reimbursement due to them, the traveler still needs to fill out a travel claim.  The details of the trip still need to be documented for auditing purposes.   All travel paperwork must be completed within 5 days of travel.
5. **No Change to this policy, but now strictly enforced** -- No conference travel expense reimbursement without proof of attendance; i.e., submit Conference Booklet or Conference Name Badge to department travel processor.

**Foreign Travel Computer Setup - Faculty, Staff, Affiliate**

When a NAU owned computer are taken out of the country the following setup procedures should be followed. The following procedures were agreed upon by the ITSS support teams and the Information Security Office.

**Standard Operating Procedure:**

* No machine leaving the country should be setup on the NAU domain. All machines leaving American soil should be treated as a "loaner" equipment.
* No encryption (BitLocker, File Vault, etc...) will be placed on any system leaving the country.
* The user of the laptop should not at any time store any sensitive documents on the computer system. All documents should be stored on one of NAU's shared file systems including but not limited to: NAUShares, Bonsai, and Dana.
* All internet communications should be performed over the NAU provided VPN.
* Upon any computer system returning to American soil, the user must immediately send the machine to ITS for a secure wipe. Any machine that has left the country for any amount of time is not to be trusted upon return.