Supplemental Information – Review of VSoE Audit Findings and Best Practices with regard to Financial Operations (August 6, 2009)

IX. Asset Management – Leticia Cornelio/Michael Goay

a. **Maintaining inventory of assets that are less than $5,000 but important to the School/Dept. (Suggest range between $1K - $5K). The basic data set should include:**
   - Location (Building/Room#)
   - User (Full Name)
   - Item make/model
   - Item serial number
   - Item description
   - Vendor (where the purchase was made)
   - Purchasing information (e.g., PO#, pcard, etc.)
   - Account
   - Date of acquisition
   - Date of last update
   - Last updated by
   - Remarks

d. **It is recommended that computer items in "good condition" be given to USC Surplus Sales see http://policies.usc.edu/policies/surplussales030107.pdf. USC Surplus Sales can ensure items are donated, disposed of, or sold in compliance with government and university regulations.**

   Be aware of the stipulations in sections 1.6 and 1.7...

   Section 1.6: RESPONSIBILITY OF UNIVERSITY EMPLOYEES WHO DO NOT USE SURPLUS SALES

   Employees who do not utilize Surplus Sales take responsibility for being in compliance with university policies and ensuring that donated, or sold items are rid of confidential information. Employees who violate university policy may be subject to disciplinary action.

   Section 1.7: DONATING / DISPOSING / SELLING ITEMS INDEPENDENT OF SURPLUS SALES

   Although donating, disposing, or selling items independent of Surplus Sales is discouraged, departments wishing to donate, dispose, or sell items to another USC department or to employees, students, or outside entities may bypass Surplus Sales. However, USC Equipment Management must be notified of all Equipment changes.

X. Information System Controls – Michael Goay

a. **Maintaining a list of all applications used to manage School/Dept operations.** The basic data set should include:
   - Application/software title (identify publisher if known)
   - System owner (if known)
   - System of records owner (e.g., University Registrar, University Payroll, department, individual, etc.)
   - System/server location (if known)
   - Software license keys (if known)
   - Functional description of the application/software
   - Vendor (if applicable, where the purchase was made)
   - Purchasing information (if applicable, PO#, pcard, etc.)
   - Account (if applicable)
   - Date of acquisition (if applicable)
   - Date of last update
   - Last updated by
   - Remarks

   Be sure to identify important freeware as well.

b. **Review and maintenance of user access levels in line with roles and responsibilities.** The basic data set should include:
   - User (Full Name)
   - System/Application
   - Scope (own record, department, school, etc.)
   - Permissions (read, modify, create, delete, all)
   - Date of action
   - Action (grant, revoke, etc.)
   - Last updated by
   - Remarks

c. **Termination of user access when employees leave university employment.** This points to the importance of maintaining accurate records as stipulated in section X.b.

d. **Password control** – changing passwords periodically (180 days); strength of passwords (minimum 6 characters and use of alphanumeric characters).

e. **System development** – user documentation; system documentation; system passwords; continuity of system programming when there is turnover in IT personnel; network configuration management and system administrator rights. This speaks to IT personnel but business managers should ensure the existence and maintenance of these documentations to support business continuity.

f. **System backup procedures and security of backup media.** Daily backup is highly recommended. If possible, encrypt the backup.

g. **Physical security of servers and hardware containing sensitive/protected information.** This shall include but not limited to desktop/laptop computers, and mobile storage devices.

h. **Saving business data on file server rather than desktop**. Most file servers are backed up daily. Server hardware resources are generally built to be more robust and offer higher fault tolerance than client computer hardware resources.

i. **Encrypting sensitive and protected data on mobile devices** (e.g., laptop computers, USB flash drives, external storage hard drives, mobile phones, etc.). Be sure to maintain encryption key escrow.