

Office of Internal Audit, Board of Regents of the University System of Georgia, (404) 657-2237

Special Interest Articles

Page 1 - Small Value Property means just that

Page 2 – Does your campus use Generic User ID's?

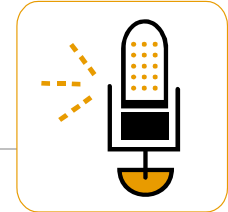
Page 3 - P-Card Audit Observations & Recommendations



“Creating A More Educated Georgia”
www.usg.edu

Words to live by:

“A Fool and his money...
...are soon audited!”



From the Desk of Ron Stark

A Happy New Year to our newsletter audience!

Tracking Small Value Property

Capital Asset items exceeding \$3,000 but not meeting Building, Infrastructure or Facilities thresholds for capitalization are not required to be tracked as SVP by institutions.

The State Accounting Office is currently developing policies and procedures for accounting aspects relating to capital assets, including SVP. If

there are any changes to the University System's current procedures as defined in the BPM as a result, these will be communicated.



Who is USER1?

Online computer systems have brought significant new capabilities to Higher Education. We are now able to register on-line, pay tuition on-line and even data mine vast amounts of sensitive data. However, putting large amounts of sensitive data on a computer and making it available on-line has also brought a new set of problems and concerns. We now need to be concerned about properly controlling access to this sensitive data.

There are two major controls that need to be implemented in any computer system which contains sensitive data: Authentication and Authorization.

Authentication is the process of ensuring that a user is really who they say they are. When a user attempts to make an entry using Banner or PeopleSoft, the system needs to be able to 1) identify the user and be able to determine, to a sufficient level of confidence, that the user is who they say they are and 2) determine what functions the user is allowed to perform.

A second REPORTS2 id was also available which provided sensitive student financial data. Since the id and password were shared, there was no method to determine who had access to the data. There was no method of determining if the user were still an employee of the institution, had recently left, or was even affiliated with the institution.

In order to protect the institution, all users must be assigned a unique id which has specific levels of authorization tied to it. The use of generic user ids provides a level of security which should not be allowed with any system containing sensitive student data.



