From the Chief Audit Officer - Outside Activities

John M. Fuchko, III

Top Ten Good Management Practices

1. Read all requests to spend University money before you sign them or approve them electronically (*Check Requests*, *Travel Authorizations*, payroll time sheets, etc.). Never sign a document unless you have reviewed at least the most important information on that document. Satisfy yourself it is a wise use of taxpayer and student funds.
2. Develop written procedures for critical operations. These serve as a resource for current employees and a good training tool for new employees.
3. Develop measurable annual department goals based on your department's mission and strategic goals. Create and action plan to achieve goals and communicate to all employees.
4. Make sure each transaction has at least two people involved: one initiator and one approver. Separate two duties to reduce the possibility of errors.
5. Print a detail transaction report from Banner once a month and review it for unusual transactions. Investigate anything that doesn't look right.
6. All cash and checks should be processed through the Cashier's Office. On the rare occasion that you do need to collect cash (this should be rare and exceptional), deposit all cash and checks received to the Cashier's Office daily. If something has to stay in your office overnight, lock it up.
7. Don't be satisfied with "the way we've always done things." Review your processes on a continuous basis for inefficiency and duplication of effort.
8. Ensure all expenditures have a clear business purpose. If the purchase is for something that *could* be construed as personal, clearly document the business purpose on the invoice or receipt.
9. Maintain good supporting documentation for all purchases. Ask yourself, "what would my supervisor or an auditor want to see?"
10. Make sure time sheets are reviewed and signed off by a supervisor or someone who is familiar with the employee's work hours.

IT Department Inundated with Problems? GSW has a Solution…

by Dean Crumbley, Tim Faircloth and Royce Hackett

You would have to be in a coma or using a Mac not to have noticed that Internet browsing today comes with increasing attempts to spy on, hijack, or otherwise infect your computer. At Georgia Southwestern State University (GSW) in Americus, Georgia, technicians have been fighting an on-going battle for the last few years, only to see more workstations infected with malware, spyware, adware, and viruses. In an attempt to combat the escalating infections and address recommendations arising from a consulting engagement performed by the Board of Regents, GSW invested in an enterprise firewall to control and manage web users, applications, and content.

In November 2009, the Office of Internal Audit and Compliance (OIAC) visited the campus of Georgia Southwestern to assess the information technology controls in place for mitigating the risks and threats associated with Identity Management, Access Control, and Network Perimeter Security. One recommendation made by the auditor recognized the need for additional technical controls and tools to monitor, identify, and mitigate threats on network segments and computer hosts. The consulting engagement report specifically noted that GSW needed to implement "an appropriate level of network content management to deter abuse or misuse of campus network bandwidth and infrastructure resources."

In order to combat the escalating number of malware infected computers and create a layer of security to mitigate web-borne threats, GSW IT management decided to invest in a web filter which would provide content filtering, application blocking, and malware protection. This web filter was purchased with the goal of supplementing existing firewall capabilities by controlling web applications, users, and content; not just ports, IP addresses, and packets.

The new web firewall was placed in-line at the campus PeachNet handoff in August 2010. Although the device is capable of acting as an "all-in-one" perimeter security solution, GSW deployed it as an additional layer of protection between the existing firewall (which already incorporated intrusion detection and prevention) and the internal network. The device was configured to block websites identified as containing malware and spyware, as well as known phishing sites. It was also set up to manage illegal peer-to-peer traffic and proxy applications.

The reduction in technical support requests concerning malware-infected machines was immediate. A review of help desk tickets revealed 95 workstations infected with malware between August - November 2009 and only 28 infected workstations during the same period in 2010, a significant reversal in the persistent trend of increasing incidents of malware infected workstations. A critical advantage of this reduction in support requests was that technical support staff could concentrate on other tasks.

"It's a huge step forward, enabling a more proactive approach to IT support," said Lynda Shaw, GSW IT support coordinator. "Technicians have been able to change their focus, allowing them to make progress on other ongoing projects, such as our migration to Microsoft Exchange."

The deployment of the network content filter resulted in an increased ability to manage the utilization of GSW computing resources. The removal of offending network activity leaves more bandwidth for legitimate purposes, resulting in better connection speeds for everyone.

IT Department Inundated with Problems? GSW has a Solution... (cont)

In addition to filtering network traffic based on the web content, this device has provided GSW

Reminder: Acceptable Methods of Federal Effort Reporting
By Chuck Fell

Tips On Spending Federal Grant Money
by Sandy Evans

Recent announcements from USG institutions have elevated community awareness and pride. Significant grants totaling millions of dollars in technical, medical, environmental, and biofuel research place Georgia in the forefront of many aspects of innovation.

Along with the grants, collaborative partnerships, and resulting recognition, the institutions need to be ready for the challenges of administrative precision in adhering to regulations, timelines, and other requirements. Amidst the euphoria of forming a technology company or winning a biomedi-

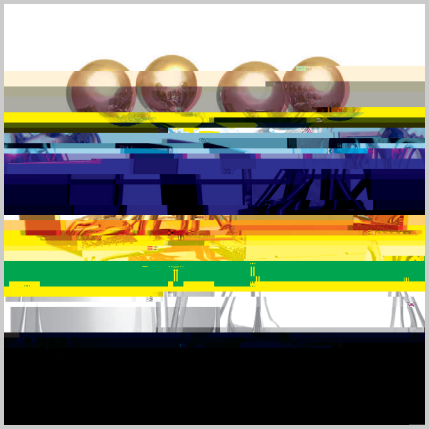
Board of Regents of the University System of Georgia
Office of Internal Audit & Compliance
270 Washington Street, SW
Atlanta, GA 30334-1450

Phone:
(404)656-2237

Fax:
(404) 463-0699

"Creating A More Educated Georgia"
www.usg.edu

We're on the Web!
See us at:
http://www.usg.edu/audit/



Ask the auditor: If you have a control or ethics question that has been bothering you, it is a good bet someone else in the system is wondering the same thing. We invite you to send your question to sandra.evans@usg.edu and we may feature it in the next or future issues of the Straight & Narrow.

Any other comments or questions?
Contact Sandra Evans at sandra.evans@usg.edu

We are looking for suggestions and feedback.