

OCR Audit Focus

A quarterly newsletter from the Office of Audit & Compliance Review

Brian Mikell, Chief Audit Executive

May, 2009

Inside this issue:

Access Request System

Cash Collections

Restricted Data Training

Access Request System for Non-*myUFL* Applications

Does your department have an information technology software application used by a variety of campus employees? Have you had trouble finding out when those employees have left the university or changed positions?

UF Bridges has developed a solution to help streamline and manage user access requests to include legacy and other applications, in addition to roles requested through the *myUFL* Access Request System (ARS).

Legacy and non-*myUFL* applications can be added to the Access Request System by Department Security Administrators. Requests will be routed to a designated approval group that consists of one or more individuals appointed to approve access to the service. Once approved, the implementation options can be manual or based on Active Directory roles automatically populated by the ARS system.

The benefits of using ARS include an automated and consolidated access request process, notification of the request itself, and documentation of both the request and approval.



Additionally, when users are terminated or change jobs within the university, automatic notifications will be sent to system security staff to let them know that access in the system should be removed. Access removal or disabling the user's access must then be manually performed unless implemented through the Active Directory interface. ARS will assist with compliance to ensure that access is limited to authorized personnel.

If you are interested in setting up your legacy or non-*myUFL* application through ARS, please contact Warren Curry, Associate Director, UF Bridges at whcurry@ufl.edu or 273-1383.

We're on the Web at:
www.oacr.ufl.edu

OACR Address:

Office of Audit &
Compliance Review
903 West University
Avenue, Room 217
P.O. Box 113025
Gainesville, FL
32611-3025

Tel: (352) 392-1391
Fax: (352) 392-3149

Editor:
Suzanne Newman
suzmcd@ufl.edu

Contributors:
Jeff Capehart
Lily Reinhart
Stan Anders

We're on the Web at:
www.oacr.ufl.edu

Unit Cash Collections

Finance and Accounting Directives and Procedures provide guidelines for the handling of cash collections. A recent audit of collection procedures at various campus units indicated that unit practices were not always aligned with university directives. Below are some reminders for handling and monitoring collections:

- Internal unit collection records should be reconciled to the general ledger using reports found in the new departmental reports in Enterprise Reporting, and not just to the commitment control reports. Reconciliations and management review of the reconciliation should be documented.
- Job duties should be properly segregated so that no single employee has complete control over

the collections process of receiving, recording, depositing and reconciling collections.

- Collection logs should document the date of receipt, check date, check number, amount and payor. Electronic check logs should be password protected to prevent changes by other employees involved in the collections process.
- Transfers of collections between employees should be documented. This would include the transfer of collections to the person delivering deposits to the Cashier's Office.

For additional information on collection procedures, please see section 1.4.11 of the Finance and Accounting Directives and Procedures website: <http://www.fa.ufl.edu/uco/handbook/handbook.asp?doc=1.4.11>

Restricted Data Training

Restricted data is data which if disclosed to unauthorized users, may have very significant adverse operational or strategic impact on an individual, a group or institution. Examples include, but are not limited to, social security numbers credit card numbers, bank account numbers, driver's license numbers, student grades, and medical records. University of Florida IT standards require anyone with access to restricted data to attend university sanctioned data protection training and to agree to comply with university data protection requirements.

Cyber Safeguards for UF Restricted Data, is provided twice a year by

the UF IT Security Team through *myUFL* training. To accommodate increased demand due to the new standards, an online version of the course is being developed and expected to be available by Fall 2009.

Additionally, UF's Identity Theft Prevention Program requires employees who have access to social security numbers to complete SSN Privacy Training which is available on the UF Privacy office website, www.privacy.ufl.edu. HIPAA training for employees with access to protected health information (PHI) and FERPA training for employees with access to student records is also available on the Privacy website.