

FINANCE ORGANIZATION SECURITY

Along with the Banner 8 upgrade, the Banner delivered 'Finance Organization (level) Security' will be enabled for querying purposes in *Banner Finance* and *LoboWeb for Finance* effective March 18, 2010.

Finance Organization Security will not impact *Finance Hyperion* and *Finance ePrint* reporting. In other words, these two reporting tools will NOT have organization level security.

Outcome

- Finance users will have Finance query access to organizations that have been requested and approved based on their business needs and requirements.
- Finance Systems Management (FSM) will collaborate with each college/school financial officer and/or fiscal agent to determine an initial base level of organization security for each respective college/school unit. A spreadsheet will be developed with this base level security and the information loaded into Banner. Additional levels of organization security required to support specific business needs will be granted through the Banner Authorization Request for security.
- Finance users will continue to have the ability to initiate, post and view all Finance documents, including Journal Vouchers (JVs), Direct Pays (DPEZs) and Purchase Requisitions (PRs) that cross all organizations.

Reasons for Change

- Lessen the exposure associated with the increasing number of computer malware, spyware and viruses that have begun to infiltrate various servers, through individual workstations, requiring a strengthening of our overall security practices, processes and protocols. In other words, protect our production database. It is important to note that individual workstations are a gateway to the applications, systems and databases that are used on a daily basis. If any of these are corrupted, all business transactions could come to a halt including payroll, purchasing and accounts payable and student disbursements. Additional information on potential risks and exposure related to malware, spyware and viruses can be found at: <http://en.wikipedia.org/wiki/Malware> or <http://en.wikipedia.org/wiki/Spyware>.
- Comply with various external compliance and regulatory requirements and in turn, protect UNM Departments from fines and penalties. Examples of recent regulatory changes: US Treasury Export Control Blacklist (strict enforcement and penalties for doing business with blacklisted countries and entities), FTC Red Flag Rules (stricter enforcement and penalties in regards to protecting identifying information) and enhanced restrictions and liability related to PCI DSS (Payment Card Industry Data Security Standards).
- Allow access to Finance forms and information that haven't been previously available.
- Facilitate easier presentation of Finance information that is relevant, meaningful, timely and appropriate to users' business needs and requirements, especially 'pushing out' information to users based on their roles using intuitive user-friendly interfaces.
- Align with organization-based security that is currently in place with Finance Budget Planner and HR/Payroll.

Planning

- For assistance and guidance on assessing departmental needs and requirements, please contact your college/school financial officer, Fiscal Agent and/or the Financial Services Division via the Financial Services Support Center (FSSC), fssc@salud.unm.edu, 277-3457.