Financial Management System (FMS) User Responsibility

As users of the FMS system, we share certain responsibilities and obligations. In addition to acknowledging the Guidelines for Responsible Computing for Montclair State University, there are important additional considerations.

The integrity of the University’s financial information is every FMS user’s responsibility. Since FMS serves as the official system of financial records for the University and the Departments for which you have responsibility, it is critically important that you do not share your system access with anyone. In the unlikely, but unfortunately possible, event that there is a suspicion of an improper financial transaction, your CWID may be implicated since each action in FMS is recorded with a CWID. When investigating the suspicious activity, the record will point to your CWID and other means will have to be used to eliminate you as a suspect in the questionable activity. Financial impropriety, in fact or in appearance, threatens the University’s reputation and continued ability to receive grants, appropriations and enjoy a favorable reputation within the financial community.

In addition to the issue of potential fraud, there is the more typical concern about financial management of the resources for which you are responsible. If others are using your system access, their mistakes are your mistakes as the system will record your CWID as the user making the entry. It is more difficult for you to document your successful budgeting, requisitioning and management skills if you allow others access to your user account.

If your user profile or your staff’s profiles are not set-up to allow the correct user to perform needed job responsibilities, you should contact the IT Service Desk at 973-655-7971, Option 2, or itservicedesk@mail.montclair.edu. They are in the position to review and redesign user profiles to best meet the needs of each user.

Please consider certain other actions that affect FMS system control and availability. Leaving your workstation unattended and logged into FMS poses a risk since someone can access your account while you are away. In addition, certain system resources are allocated to each user that is logged into FMS, thereby limiting the access of other FMS users since system resources are limited.

Finally, FMS staff depends on your communication of changes in personnel or in responsibility of existing staff. If staff moves and they had FMS access to a Department for which you are the responsible person, it is possible that they will still have access unless you notify the IT Service Desk, that the user should no longer have such access.

Thank you for your attention to these critical security issues of FMS.

Donald D. Cipullo
VP for Finance and Treasurer

(8-21-15)