

City of Miami Beach, 1700 Convention Center Drive, Miami Beach, Florida 33139, www.miamibeachfl.gov
Office of Internal Audit
Tel: 305-673-7020

TO: Margarita Wells, Environment and Sustainability Department Director

VIA: Mark Coolidge, Assistant Internal Auditor *MC*

FROM: Fidel Miranda

DATE: September 30, 2017

SUBJECT: **Assessment of Access Rights for EnerGov User Roles (Environment and Sustainability Department)**

Meetings were held with pertinent Environment and Sustainability Department staff to review and assess the risks associated with created EnerGov user roles and the corresponding access rights and privileges granted to its employees. A copy of the corresponding "EnerGov User Role Access Audit Report" is attached that details the access rights granted to employees as a result of these meetings.

The focus of this review was to identify instances whereby these user roles and/or corresponding system accesses granted could have an adverse impact on segregations of duties and/or internal controls. One (1) user role entitled "Environmental Sustain" was identified that granted access to four departmental users. The user role's naming convention was established by the Environment and Sustainability Department in conjunction with the Information Technology Department so it was not changed to help avoid creating any confusion.

Only one (1) user role can be assigned to each staff member; however, all employees assigned under a user role will share the same system accesses and privileges. In other words, department users have a one to one relationship to user roles, while user roles have a one to many relationship to department users.

After reviewing the access rights and privileges granted to the "Environmental Sustain" user role, it was noted that the following items are in need of further consideration, which have been highlighted on the "User Role Access Report" presented after this memo.

- a) The ability to adjust fees (AllowAdjustFees)
- b) The ability to delete attachments to the file (AllowDeleteAttachment)
- c) The ability to void invoices (AllowVoidInvoices)
- d) The ability to edit invoices after being created (AllowInvoiceEditing)
- e) The ability to skip, approve, and create steps and actions in workflow (AllowWorkflowManagement)
- f) The ability to create, delete, alter, approve, etc. workflows (WorkFlowAdministrator)

Due to the relatively small number of clerical staff, all employees need to have the same access as they substitute for one another when someone is out of the office. Although necessary, this scenario poses a greater risk since segregations of duties is minimal.

In addition, the department should consider implementing a continuous monitoring program by an employee independent of the changes to the security options and rights described above. An "Exceptions Report" has been created by the Information Technology Department to help identify all instances whereby any of these actions took place to facilitate reviewing their validity.

In addition, Environment and Sustainability Department management should consider removing the ability to edit invoice information once the invoice has been created. Any subsequent edits will create discrepancies between the information reflected on the invoice and in EnerGov. Instead, it is recommended to void the invoice in these instances and make the proper corrections in the system to ensure agreement between the information recorded electronically and the physical document.

Furthermore, allowing users the ability to delete attachments in the system should be reconsidered. It is important to note that attachments provide the supporting documentation required for the work performed. In addition, there are record retention requirements that must be complied with, which users may not be aware of. Although we view the ability to remove attachments as a lesser risk, its granting merits closer consideration.

Moreover, it is recommended that the workflows created properly align to the business processes and rules already implemented through the department's Standard Operating Procedures. This practice will help allow for the creation of meaningful workflows that will reduce the need for any user to have access to change and/or skip any steps of the established process. The rights to manage and/or administer workflows should be maintained at a System Administrator level and not by system users.

F:\OBPI\AUD\INTERNAL AUDIT FILES\DOC16-17\PC WORK\EnerGov Roles & Rights\Pubic Works 7-20-17\Word Versions\Audit Memo 09-30-17 - Environmental.docx

cc: Susanne Torriente, Assistant City Manager
Mark Taxis, Assistant City Manager
John Woodruff, Chief Financial Officer
Ariel Sosa, Director – Information Technology Department