MIAMIBEACH

MEMORANDUM

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

TO: John Woodruff, Chief Financial Officer

VIA: Mark Coolidge, Assistant Internal Auditor MC

FROM: Fidel Miranda

DATE: September 30, 2017

SUBJECT: **Assessment of Access Rights for EnerGov User Roles**

The purpose of this memorandum is to provide an update regarding the status of Internal Audit's review of the Information Technology (I.T.) Department's assigned EnerGov user roles at the request of each applicable department/division director. Meetings were held and the created user roles reviewed for the corresponding nine (9) departments/divisions. During this process, we have assisted these departments/divisions to establish the requirements of each user role and have allowed time for operations to assess whether the recommended accesses and settings under each user role created actually allow the users to still perform their assigned job duties.

Once the user roles are tested and agree upon, the current settings for each user role is emailed to the corresponding Director to affirm along with any specific observations and recommendations. One general rule is that no user roles should be allowed the ability to delete records from the system or perform any function that may affect the completeness and reliability of historical data and audit trails.

The following user roles and/or corresponding system accesses granted could have an adverse impact on segregations of duties and/or internal controls:

- A process to create new user roles and/or modify any existing user roles after being confirmed by the department/division director at the end of our review should be established, implemented and continuously followed. Currently, an e-mail or a phone call from a Director or his/her designee is sufficient to initiate a change. A new process should be implemented whereby supporting documentation is maintained detailing the reasons for the change which contains the Director's signature as they are the ones responsible for certifying final roles, accesses and the individuals assigned to each role. Once complete, the request should be routed to the corresponding Assistant City Manager or City Manager to assess internal controls before the change is forwarded to the I.T. Department for execution. This process should be followed consistently going forward for all additions, deletions or revisions to access controls, user roles and the employees assigned.

- The need for an "Exceptions" report was discussed with the I.T. Department which would capture areas like fee deletions, fee adjustments, workflow skipping, workflow deletions and/or editing, invoice adjustments, voiding invoices and any other information useful for the supervision and review of the department's transactions and/or system interactions. The report should include the explanation for the transaction and the preparer's name plus the information both before and after the change (What it was vs. what it is now). This report should be used by departments/divisions for review, supervision and as a risk mitigating internal control considering that it provides the required audit trails.

- There seems to be lack of understanding by the software users regarding the options, operations, and capabilities of the EnerGov software. Additional training should be required of all EnerGov

users to facilitate the learning and familiarization with the software capabilities in their corresponding disciplines.

- Occasionally, there may be a need for many user rights and capabilities assigned to a particular user role (especially in small departments/divisions where job duties often overlap). In these cases, the potential risks associated with user rights can be mitigated by establishing controls and review processes, as part of the business processes and process workflow within the departments/divisions. As a result, one should test the effectiveness of internal controls, both in design and practice for every EnerGov user department/division by looking further into their processes and business rules, once this review is complete. This practice will help to close any gaps identified between user access rights and user roles in the different processes.

- All user roles provided with the following security options and should be frequently monitored:

    1. AllowAdjustFees
    2. AllowDeleteFees
    3. AllowWorkflowManagement
    4. WorkflowAdministrator
    5. AllowInvoiceEditing

  Allowing any user the ability to adjust fees, delete fees and/or edit invoices after being created poses a risk for unscrupulous behavior, as well as for inadvertent mistakes and entries; all of which could result in reconciliation differences between balances reflected in EnerGov, the physical invoice and/or in MUNIS. Departments/divisions with user roles having these privileges should implement business processes to frequently review audit trails to determine the adequacy of transactions. In addition, an approval process for fee adjustment, fee deletion and/or invoice editing should be created and followed consistently.

  Allowing users to manage and administer workflows poses a risk to the fundamental operations and processes within the departments/divisions as workflow management and administration should be kept at a system administrator's level. Having this access allows a user to add or delete steps and actions to a process; pass or fail steps and actions in a process; redo, re-prioritize, and skip steps and actions in a process; etc. Workflows are designed and developed to establish actions and steps that are driven by the Standard Operating Procedures and business rules approved and implemented by each department/division. Any changes in workflow should be documented by revised or newly established and approved procedures. Best practices should be to review the current business processes and map it out so that creating the workflow is easier. Once created, no individual user should have access to alter or bypass any step or action as this would be a departure from the established business processes.

- Every time additional forms/modules are created in EnerGov, all users get full access including the right to delete, which should be prevented whenever possible. This practice requires continuous review by the I.T. Department administrator to ensure additional access is not granted to users without following the review process for changes. Consequently, it should be discussed with the software vendor to determine whether the system can be programed to initially deny access to all users unless proper documentation and process adherence to grant access is received.

- No controls are currently in place to document or monitor changes and/or additions initiated and/or performed by the I.T. Department's system administrators. In addition, no restrictions with respect to access to operational modules have been established. As a result, a system administrator can create, make changes to, and/or delete user roles, assign and/or un-assign users to user roles, design, develop and/or delete workflows, among other privileges, without an internal review and authorization process. Consequently, limiting and documenting the roles and accesses granted to system administrators is recommended as they should not have access to

actual production records and forms, or the ability to change records and data in the production environment. Audit trails should be identified, established and monitored for any actions taken by a system administrator to ensure adherence to the documentation, review, and approval processes and requirements as implemented by the I.T. Department.

- Financial transactions and/or fees recorded in EnerGov do not automatically synchronize with MUNIS which could result in reconciliation discrepancies between the two systems. Options for integration and automatic synchronization should be explored to minimize reconciliation discrepancies especially since both systems were developed by the same vendor (Tyler Technologies).

These areas identified, for which additional attention and review is recommended, represent general observations to mitigate risks associated to the use of the EnerGov system. More specific observations and/or recommendations are being reported separately to each affected department/division for their review, consideration and action.

F:\OBPI\$AUD\INTERNAL AUDIT FILES\DOC16-17\PC WORK\EnerGov Roles & Rights\Audit Memo All 09-30-17.docx

cc: Mark Taxis, Assistant City Manager
Ariel Sosa, Director – Information Technology Department