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: Virgilio Fernandez, Fire Chief

VIA: Mark Coolidge, Assistant Internal Auditor MC

FROM: Fidel Miranda

DATE: September 30, 2017

SUBJECT: **Assessment of Access Rights for EnerGov User Roles (Fire Department)**

Meetings were held with pertinent Fire Department staff to review and assess the risks associated with created EnerGov user roles and the corresponding access rights and privileges granted to employees. A copy of the Fire Department's "EnerGov User Role Access Audit Reports" is attached that detail the access rights granted to staff 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. The six (6) EnerGov user roles listed below were created to grant access to the listed number of Fire Department assigned users. The naming conventions were established by the Fire Department in conjunction with the Information Technology Department so they were not changed to help avoid creating any confusion.

- Fire Annual Inspections – (8 users)
- Fire Annual Insp Sup – (1 user)
- Fire Inspect Review – (7 users)
- Fire SM Escalate/InspRevu – (1 user)
- Fire Supervisor – (6 users)
- Fire Supervisor Backup (1 user)

The following two (2) additional user roles were also created but have no individuals assigned and therefore should be deleted:

- Fire Annual InspectorsOLD
- Fire Supv

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

After reviewing the access rights and privileges granted to each of the six (6) EnerGov user roles with assigned users, it was noted that the following items are in need of further consideration, which have been highlighted on the "EnerGov User Role Access Audit Reports" presented after this memo.

1. Users under the “Fire Annual Inspectors” User Role have been granted, among others, the Following Security options:

    a) AllowDeleteAttachment – This access allows users to delete attachments from records, even after they have been uploaded and saved onto the system.
    b) AllowHoldOverrides – This access allows users to override holds placed on activities such as inspections, plan reviews, etc.
    c) AllowWorkflowManagement – This access allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
    d) InspectionSecurityAdministrator – This access allows users to assign inspectors and/or change statuses in Manage My Inspections for inspections that have not been assigned to these users.

    Users assigned to this user role are mainly Fire Inspectors and removing these rights and accesses are recommended as they were also given to their higher ranking supervisors. In addition, all of these privileges should be kept at higher position levels to ensure compliance to standard operating procedures, documentation requirement guidelines, and to provide better segregation of duties, as well as checks and balances.

2. The “Fire Annual Insp Sup” user role grants its assigned users the following security options among others:

    a) AllowWorkflowManagement – This access allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
    b) WorkFlowAdministrator – This access allows users to add steps and actions; re-prioritize and sort workflow; delete steps and actions; skip steps and actions; receive steps and actions; pass / complete steps and actions; fail steps and actions; redo steps and actions; and fetch on demand steps and actions within a process.

    Although a report can be generated to identify all instances in which a workflow step was bypassed, it would require continuous monitoring to detect any incidents whereby a step or an action is skipped or approved through the workflow. Instead, best practices would be to map out the current business processes so that creating the workflow is easier and each required step or action is given the adequate hierarchy in the workflow; therefore, removing the need to allow access to any user role to manage the workflow. Once created, no individual user should have access to alter or bypass any step or action, as this would be a departure from the business processes.

    Workflow management should be a procedural control and not an operational option. Consequently, Internal Audit recommends ensuring that workflows are created to reflect the processes of the department and once properly set up that only System Administrator level users should have access to manage or administer workflows. Workflows should be the result of Standard Operating Procedures and established business rules within the department.

3. Users under "Fire Inspect Review" user role have been granted the following security options:

   a) AllowHoldOverrides – This access allows users to override holds placed on activities such as inspections, plan reviews, etc.
   b) AllowWorkflowManagement – This access allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
   c) WorkFlowAdministrator – This access allows users to add steps and actions; re-prioritize and sort workflow; delete steps and actions; skip steps and actions; receive steps and actions; pass / complete steps and actions; fail steps and actions; redo steps and actions; and fetch on demand steps and actions within a process.

   Holds are usually placed in a process to prevent the process from moving forward due to pending fees, inspections, incomplete documents, etc. This privilege has been provided to other higher ranking users and user roles in the Fire Department and it should only be used when holds are unrelated and do not affect the processes. However, developing proper workflows for the different processes should also help resolve this problem and take away the need for this system right. Usually if the hold is placed, then it is meant to delay all processes and to provide the City better leverage in resolving whatever is pending. As mentioned previously in finding #2, the "AllowWorkflowManagement" and "WorkFlowAdministrator" rights should not be assigned to this user role.

4. Users under the "Fire SM Escalate/InspRevu" user role have been granted the following security options which should be removed:

   a) AllowWorkflowManagement – This access allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
   b) WorkFlowAdministrator – This access allows users to add steps and actions; re-prioritize and sort workflow; delete steps and actions; skip steps and actions; receive steps and actions; pass / complete steps and actions; fail steps and actions; redo steps and actions; and fetch on demand steps and actions within a process.

5. The "Fire Supervisor" user role grants assigned Fire Department employees the following access and security options:

   a) Business License / License Viewer/Rapid License Renewal/Delete – Allows users' access to the screens where they could add, update, or delete Rapid License Renewal.
   b) AllowDeleteFees – Allows users the ability to delete fees.
   c) AllowWorkflowManagement – Allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
   d) WorkFlowAdministrator – This access allows users to add steps and actions; re-prioritize and sort workflow; delete steps and actions; skip steps and actions; receive steps and actions; pass / complete steps and actions; fail steps and actions; redo steps and actions; and fetch on demand steps and actions within a process.

Internal Audit recommends removing rights allowing users to delete information from the system whenever possible. Fire Supervisors may need access to add and update license renewals; however, the right to delete them should be reviewed and revised to be removed. If it is imperative for this user role to have the right to delete information, then adequate internal controls and departmental processes should be established to ensure a proactive monitoring process to detect any errors, unnecessary or insufficiently documented deletions.

The same should be considered for the right to delete fees as fees can be adjusted without the need to be deleted. However, if the department feels that the need to delete fees is necessary for their course of business, the adequate processes and controls should be implemented procedurally to detect and/or avoid errors and/or unauthorized deletions Lastly, the "AllowWorkflowManagement" and "WorkFlowAdministrator" rights should not be assigned to this user role as mentioned previously.

6. Users under "Fire Supervisor Backup" have been granted the following security options which should be removed:

   a) AllowWorkflowManagement – This access allows users to add steps and actions in a process; receive steps and actions; pass/complete steps and actions; fail steps and actions; redo steps and actions; and fetch On Demand steps and actions.
   b) WorkFlowAdministrator – This access allows users to add steps and actions; re-prioritize and sort workflow; delete steps and actions; skip steps and actions; receive steps and actions; pass / complete steps and actions; fail steps and actions; redo steps and actions; and fetch on demand steps and actions within a process.

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

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