

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

TO: Thomas Mooney, Planning Department Director

VIA: Mark D. Coolidge, Interim Internal Auditor *MDC*

FROM: Norman Blaiotta, Senior Auditor *NB*

DATE: January 16, 2018

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

Internal Audit has assessed the risks associated with created EnerGov user roles and the corresponding access rights and privileges granted to Planning Department employees. 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. Copies of the "EnerGov User Role Audit Reports" were separately presented to Planning Department management detailing the access rights granted to pertinent staff.

The eight (8) EnerGov user roles below were created to grant access to the listed number of assigned users. The naming conventions were established by the Planning Department in conjunction with the Information Technology Department so they were not changed to help avoid creating any confusion.

1. Plan-Admin (8 users)
2. Plan-Admin Parking (2 users)
3. Plan-AdminWCap (1 user)
4. Plan-Inspector (2 users)
5. Plan-Reviewer (11 users)
6. Plan-Reviewer/Inspect (2 users)
7. Plan-Supv 1 (5 users)
8. Plan-Supv 2 (3 users)

In addition, the following two (2) additional user roles were also created but have no individuals assigned and therefore should be deleted if they are not going to be used:

1. Plan WF/PR/Fee/INSP SUPV
2. Plan-Data Entry

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, departmental users have a one to one relationship to user roles, while user roles have a one to many relationship to department users.

Testing found that all individuals included in the following seven (7) Planning Department user roles were given access to the AllowWorkflowManagement and WorkFlowAdministrator user

roles were given access to the AllowWorkflowManagement and WorkFlowAdministrator user rights as highlighted on the separately presented “EnerGov User Role Audit Reports”:

1. Plan-Admin
2. Plan-Admin Parking
3. Plan-AdminWCap
4. Plan-Reviewer
5. Plan-Reviewer/Inspect
6. Plan-Supv 1
7. Plan-Supv 2

AllowWorkflowManagement grants assigned users the ability to bypass steps or actions in the workflow for a particular record, as well as create steps and actions in a pre-established workflow. Meanwhile, WorkFlowAdministrator allows users the ability to create, delete, alter and approve workflows. Allowing users to manage and administer workflows poses a risk to the fundamental operations and processes within the department as it is recommended that it be kept at a System Administrator's level.

EnerGov's User Setup Manual defines the function of a System Administrator as "Allows the user to perform the same functions as AllowWorkflowAdministrator". By definition, System Administrator is the most comprehensive access right in any system so that anyone granted the AllowWorkflowAdministrator access has in fact a System Administrator access role. As a result, it is recommended to remove both the AllowWorkflowManagement and the AllowWorkflowAdministrator rights from everyone but the actual System Administrator.

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, individual users should not have access to alter or bypass any step or action as this would be a departure from the established business processes.

Lastly, the table shown below lists ex-City employees whose rights within the reviewed Planning Department user roles were not terminated timely according to the “EnerGov User Role Audit Reports” created on 11/07/2017.

Ex- City Employee ID #/Name	User Role	Termination Date	Number of Days Between 11/07/2017 and Termination Date
16194	Plan-Admin	08/22/2017	77
Sarai Alvarez (Temp)	Plan-Admin	06/16/2017	144
20658	Plan-Reviewer	03/24/2017	228
20759	Plan-Admin	06/30/2016	495

Planning Department's Management Responses and Internal Audit Observations

Upon receipt of this assessment's initial draft report, the Deputy Planning Director emailed a response to the issues expressed. A meeting to discuss these responses was subsequently held with the Deputy Planning Director and the Information Technology (IT) Department personnel responsible for maintaining the EnerGov system. The four (4) items discussed in this meeting are listed below along with the Planning Department's position on each of these issues as well as Internal Audit's Observations which provide additional detail or clarification.

1. Naming conventions utilized in this report.

Planning Department's Response:

The naming convention accurately represents the functions of the role. There is no need for modification at this time.

Internal Audit's Observation:

This assessment neither requires nor suggests changes to the naming convention. The phrase only explains the source of the naming convention and the reason why it was not considered for revision.

2. Existing user roles with no individuals assigned should be deleted if they are not going to be used.

Planning Department's Response:

"Plan WF PR Fee INSP SUPV" was created by the Tyler team during the go-live to facilitate implementation of the new software until the User Roles were further refined. "Plan-Data Entry" was created by the Department to be used by Temporary Staff for data entry purposes only. The role is currently not in use, but it is likely to be used again in the future. Please be advised, that once created and used, User Roles cannot be deleted from the system; they simply become dormant while not in use since no one is assigned to it. The ability to reuse a User Role also allows for the efficient use of the system since Planning Staff and the System Administrator do not have to re-create User Role multiple times as the need arises.

Internal Audit's Observation:

Different from users, user roles can be deleted from the EnerGov system and there are no repercussions from removing them as verified with IT staff. However, since the risk involved in keeping unused user roles is minimal, there is no objection to the Planning Department's position.

3. Allow users to manage and administer workflows through the AllowWorkflowManagement and WorkFlowAdministrator user roles.

Planning Department's Response:

It would be inefficient to create a workflow for each different path an application could take. Additionally, were it not for the authorities granted under the AllowWorkflowManagement

and WorkflowAdministrator, applications could not move forward as the members of the staff could not create additional (pre-established) steps, skip unnecessary steps, and alter steps which allow the user to reorder steps in a workflow as needed. Additionally, while establishing our user roles with the System Administrator, we requested that no access be granted to "delete" items in the workflow regardless of User Role. If you find otherwise, please advise so we can make the necessary request for modification. Please also consider that "The System Administrator" resides in the IT Department. That person(s) does not manage or oversee Planning Department functions. It would be inefficient and cumbersome to request the IT System Administrator to modify a workflow of a business process under the purview of the Planning Department.

Even though we are fortunate to have an exemplary professional staff, we are confident that you are aware that EnerGov provides an extensive audit trail. This audit trail, which cannot even be altered by the CMB System Administrator, documents and memorializes any changes to the records; inclusive of changes to the workflows.

Internal Audit's Observation:

The Office of Internal Audit (OIA) discussed with IT personnel the details on how EnerGov was configured and the requirement of Planning Department's employees to skip steps in the workflow during their daily work tasks. The IT personnel explained that the right to skip and/or delete steps in the workflow is granted only by the AllowWorkflowAdministrator role which is a security concern if other compensating controls are not created and followed. Furthermore, there is no known means to separate the ability to skip and delete steps due to current EnerGov system limitations as access is currently restricted to either both or none.

The OIA also asked why the granted AllowWorkflowManagement role cannot be used to pass a step, instead of skipping or deleting it in the workflow, which is not allowed in the aforementioned role. The IT personnel responded no, since pass refers to a step that was fulfilled.

The Planning Department statement that an extensive audit trail is provided by the system to record changes is accurate. Yet, it is important to note that the audit trail records the system's activity, but is not able to prevent irregularities and it requires routine reviews of transactions by an individual(s) independent of these user roles to be most effective. Of all the post log-in security options a system may offer, audit trails should not be considered a first, or unique, line of defense, but the last.

Although this assessment is focused on promoting a proactive (preventive) approach on the EnerGov system's security instead of a reactive one, the OIA realize the necessity of Planning Department employees to skip steps based on current's system configuration. As a result, the OIA believes that a documented monitoring process be performed consistently by Planning Department management by continuously reviewing exception reports sourced from the audit trail. This practice should also be accompanied by the creation of a Standard Operating Procedure which will include, but not be limited to, a listing of designated personnel responsible to perform the review and their back-ups as well as the frequency and the methodology to be used.

4. Ex-City employees whose EnerGov rights were still active in Planning Department's user roles.

Planning Department's Response:

The System Administrator is under IT, and is responsible for the deactivation of any Users in the EnerGov system. This matter should be raised with the IT Department directly since it is our understanding that they do not deactivate Users in EnerGov until advised to do so by the Department of Human Resources. Please also consider that users cannot be "deleted" from the system, they are just deactivated and that some time must pass between separation and deactivation to allow for the reassignment of work. Additionally, EnerGov uses the CMB User name and password protocols to allow access. Once network access is terminated, the employee cannot access EnerGov.

Internal Audit's Observation:

The word "delete" was neither included nor implied in this assessment. The System Administrator is responsible to deactivate users as directed by the Human Resources Department. Testing confirmed that three of the four ex-Planning Department employees were deactivated from the network timely upon written request from the Human Resources Department. However, IT was unable to provide documentation indicating when they were requested to deactivate employee identification number 20759 from the network so no conclusions could be reached in this case.

Although we agree that the compensating control is the prompt removal of the user's network access, there is unfortunately no guarantee that this step will be timely performed as it may not be requested by Human Resources or acted upon by IT. Similarly, there is a remote possibility that an ex-employee could improperly access the EnerGov system through a current employee's unattended computer. Therefore, OIA maintains that the preferred approach is to have IT timely deactivate a terminated employee's access to both the network and the EnerGov system to sufficiently reduce the risk of unauthorized usage.

F:\OBPI\AUD\INTERNAL AUDIT FILES\DOC17-18\REPORTS - FINAL\Audit Memo - Planning 01-16-18 (EnerGov).docx

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