

SOP for User Access Review
August 26, 2010

Author: Duke Arakaki

Approved By: IT Planning and Administration

Revision	Date	Responsible Person	Description of Change

Recertified:

Initials				
Date	xx/xx/2011	xx/xx/2012	xx/xx/2013	xx/xx/2014

Table of Contents

Purpose and Scope:	3
Procedure:	3
Roles and Responsibilities:	4
Reference:	4

Purpose and Scope:

This IT Standard Operating Procedure (SOP) describes the procedure for reviewing City of Roseville user accounts for the application data management systems. This SOP is applicable when a user joins or leaves the organization, or the user's role requires a change to access to a data management system. Adherence to this SOP protects the security, privacy and data integrity of City of Roseville data in the systems.

It applies to all City of Roseville Employees who use City applications containing financial and sensitive data. These applications may include or exclude any city application. Some examples of included applications would be Banner-Utility Billing, IFAS-Finance, Class/GeN-Parks, and Envisionware/STS-Library.

Roles and Responsibilities:

Employee

- Will coordinate application level of access with supervisor based on role and needs.

Employee's Supervisors (Primary responsible for the day to day management of employee and access use for each system.)

- Will request access for their employees from the Application Administrator and determine the user's appropriate level of access or role in accessing the application.
- In the case of accidental removal from necessary applications, the employee's supervisor must notify the Application Administrator of the need for access.
- Should contact the Application Administrator of employee's status changes, or their work responsibilities related to specific applications that are completed or change.

Application Administrator (Responsible for reviewing applications and determining access need meets request)

- Notify IT Service Desk when an employee's status changes, or their work responsibilities related to specific application are completed or changed.
- Will coordinate with employee's supervisor to verify the level of access to the application data management system is appropriate to the level the user needs to perform job functions.

Business Analyst (IT staff who is responsible for application support)

- Create and modify user accounts under direction of Application Administrator.

IT Service Desk (IT staff responsible for first line of support)

- Create ticket from Application Administrator's request.

Procedure:

1. Business Analyst will provide each department with a list of users denoting permissions for their application.
2. A review of user access and privileges will be conducted annually in March and September by the Application Administrator.
3. If a user account for a terminated employee is discovered in the audit, the terminated employee's account should be immediately removed or suspended. The employee's supervisor will send employee termination information such as employee name and termination date to Application Administrator and the IT Service Desk immediately.
4. If a user account is deemed to have inappropriate permissions, the Application Administrator will immediately notify IT Service Desk to disable the account in question until further investigation is completed within 2 business days. Upon conclusion of the investigation, Application Administrator will provide correct privileges to IT Service Desk based on the results of the findings.
5. Responsibility of user access verification is the responsibility of the requesting supervisors and Application Administrators. The Application Administrator will work with departmental supervisors regarding their employee's access.
6. In the case of accidental removal from necessary applications, the employee's supervisor must notify the Application Administrator (see Employee Supervisors Roles and Responsibilities).

Reference:

None.