Policy Type: Administrative

Category: Fiscal and Budget

Policy Name: Maintaining Kronos User Security

Policy Owner: Controller-Treasurer Department

Policy Purpose

The purpose of this policy is to ensure that County departments protect information stored in Kronos, the County's timekeeping software, as well as follow the Kronos Security Policy and allow only designated staff members access Kronos information.

Policy Summary

Access for each Kronos user must be approved by the user's manager and the Kronos Systems Administrator. Each user will be assigned a unique User ID number.

A user can request access to Kronos by submitted a completed, approved **Kronos Security Access Request Form** to add, change, or delete user data in Kronos. Such requests should be addressed to the Controller-Treasurer Department Systems Unit.

All Kronos users must follow this policy, as well as the **Kronos Security Policy**, which is available at
[url]
/sites/forms/Kronos/KronosCountywideForms/Kronos%20Security%20Access%20and%20Policy.pdf.

Additionally, all Kronos users must agree and adhere to the Santa Clara County Information Technology User Responsibility Statement.

Concurrent Kronos and Human Resources Payroll System Access

Kronos users with concurrent access to the Human Resources Payroll system (HaRP) shall be limited to "view-only" access in HaRP unless:

1. Internal/compensating controls are in place to mitigate the risk of update capability in both systems, and

2. The user's job duties require update capability in both systems and there are no reasonable alternatives to the concurrent access levels

Procedures

Creating a New Kronos User

1) Upon identifying an employee with a legitimate business need to access Kronos, the **department** completes the Kronos Security Access Request Form, including filling in the employee's name, department, Kronos access level requested, and any other necessary information on the form.

2) The **departmental Kronos security coordinator** approves and dates the Kronos Security Access Request Form and submits it to the Kronos Security Administrator.

3) If the Kronos access level requested includes the authority to approve timecards, the **Controller-Treasurer Department Systems Division** checks to see if the user has an account with the Human Resources Payroll (HaRP) system (PeopleSoft) with the ability to hire.

3a) The **Controller-Treasurer Department Systems Division** conducts a PeopleSoft query for the user with query "SEC_SC_PS8_OP_ABILITY_TO_HIRE".

3b) If the user has the ability to hire, the **Controller-Treasurer Department Systems Division** notifies the department of the restrictions explained above.

3c) If necessary, the **department** completes another Kronos Security Access Request Form.

4) Upon verifying that a user does not have concurrent access or that the limited exception described above is met, the **Controller-Treasurer Department Systems Division** logs into Kronos and sets up the new user account with rights as specified on the Kronos Security Access Request Form.

5) The **Controller-Treasurer Department Systems Division** contacts the new Kronos user and informs the user of his or her Kronos user name, password, and "close of pay" check-off lists.

6) The **Controller-Treasurer Department Systems Division** files the Kronos Security Access Request Form.

Managing Kronos User Access

1) Every two weeks, the **Controller-Treasurer Department Systems Division** runs Genie of "SCC Mgr Appr or TK" and compares the Organizational Group with TCN/BU for transferred employees. The **Kronos Systems Administrator** removes access for users whose organizational Group does not belong to TCN/BU.

2) Quarterly, the Kronos Systems Administrator runs WIM import "Users Last Logon Audit" on server "sccsvtkprd70" to get the last log on date for active employees with manager licenses. The **Kronos Systems Administrator** inactivates Kronos manager accounts for users who have not logged on for at least one year.

Definitions

For the purposes of this policy, the following definitions apply:

1) "**HaRP**" means the Human Resource Payroll system currently used in the County of Santa Clara.

2) "**Kronos**" means the County's current employee timekeeping software program.

Frequently Asked Questions

None.

Related Policies

- Information Technology User Responsibility Statement - https://iservices.sccgov.org/sccurds
- Maintaining HaRP User Security - https://saecommon.sccgov.org/countypolicy/Maintaining-HaRP-User-Security.pdf

Related Forms and Information

- Kronos Security Policy and Security Access Request Form – [url] /sites/forms/Kronos/KronosCountywideForms/Kronos%20Security%20Access%20and%20Policy.pdf

History

Date	Changes Made
10/05/2017	Links updated. (David Bruno)
2/13/2015	Form updated. (John Myers)
9/18/2014	Policy Uploaded. (Kyle Larson)