STANISLAUS COUNTY COMMUNITY SERVICES AGENCY	Developed by/Date: Security Workgroup 4/08, 7/10	Page: 1 of 3	Number: 7.21
			Subject: Administrative
	Reviewed by/Reviewed Date: Exec Committee 4/08, 7/10	Replaces:	Distribution: Leadership
Title: **Internal Audit Request**		Approved: 8/2/10	

Policy ☑ **Procedure** ☑ **Guideline** ☐

Purpose

This policy has been established to standardize and streamline new and current procedures for Management to request information from various resources related to employee work activity. These procedures will also facilitate appropriate notification of Human Resources and Division Heads.

Procedure

A. Audit requests should be made through the HR Manager (unless otherwise specified in this policy) via an email or telephone call, and need to include a brief explanation of the reason for the request. The HR Manager will determine whether there is an appropriate and legitimate business need to retrieve the information.

B. Internal Audit Reports available upon request:

1. Access Card (Badge) System Request

   This request will produce a report which provides a record of an individual employee's access to all secured doors by date and time. The report can also provide information specific to each door which has a reader.

2. Cell Phone Usage Audit Request

   The request will produce a report which provides a record of an individual employee's calls made by date and time for the most recent billing period.

3. C-IV Security Audit Request

   C-IV usage reports are generated both randomly and upon request when there is an appropriate and legitimate business need to determine who has accessed a case or what case(s) a user has accessed. Reports will be reviewed for possible security violations. A C-IV Security Violation memo detailing the findings will be sent to the HR Manager.

4. Equipment Audit Request

   The request will produce a report which provides a list of all CSA equipment checked out to an individual employee. Equipment audit requests should be made through the IT Department via a technical work request; include a brief explanation of the reason for the request. Equipment audits do not include county credit cards.

   Equipment that may be audited includes but is not limited to:

   a. Cell Phones / Blackberries
   b. Laptops
   c. Wireless Cards
   d. PDA (Palm's)
   e. Pagers

5. GroupWise Email and GroupWise Messenger Audit Request

   The request will produce a summarized list of emails and/or messages sent and received by an individual employee or a detailed list of actual emails and messages.

   CSA retains all email and Messenger communications for 6 months. These communications can be retrieved and viewed for appropriate and legitimate business reasons.

6. Internal Investigation Request

   Requests for internal investigations should be made through the HR Manager or the SIU Chief via email or a telephone call; include a brief explanation of the reason for the request. The HR Manager or SIU Chief will determine whether there is an appropriate and legitimate business need to conduct an investigation.

7. Internet Usage Request

   Internet usage reports are generated monthly by IT for all employees with excessive Internet usage during the preceding month or have visited inappropriate internet sites. These reports are reviewed by IT for appropriate Internet usage as outlined in the IT Security Policy signed by all CSA employees.

8. Remote Access Audit Request

   The request will produce a report which provides limited information regarding when a specified user has logged into the system.

9. Video and/or other electronic surveillance.

   Review of existing surveillance or requests for new surveillance should be addressed with the HR Manager. The HR Manager will work directly with the Department Head, the Assistant Director, and consult with SIU Chief and County Counsel on these requests.

10. Wireless Card Usage Audit Request

    The request will produce a report which indicates the amount of data transferred for the most recent billing period.

C. Exceptions to this policy may be required for agency security.