The California State University
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4201
(562) 951-4412

Date: May 5, 2003

Code: **TECHNICAL LETTER**
HR/Personnel Records 2003-01

To: CIRS Security Coordinators

Time Sensitive:
Forms due May 23, 2003

Cathy Robinson

From: Cathy Robinson, Assistant Vice Chancellor
Human Resources Administration

Subject: **Protection of Confidential Information from the Campus Information Retrieval System (CIRS)**

In light of recent concerns regarding data confidentiality and the potential of identity theft, we want to take the opportunity to remind our CIRS Security Coordinators of their responsibilities and provide clarification on required forms relating to protecting confidential employee data. As you are aware, CIRS is the systemwide data warehouse for human resources information, available to all campuses as well as the Chancellor's Office, developed and maintained by our Human Resources, Information Support and Analysis (HR-ISA) staff in Sacramento. The following information also can be found on the CIRS Web site at http://www.calstate.edu/hrpims.

CIRS Security Coordinator Duties

The campus is responsible for data security and CIRS access. CIRS Security Coordinators are responsible for authorizing CIRS access and monitoring data security and equipment. CIRS Security Coordinators are the primary CIRS campus contact and have the following duties:

- Signing and overseeing completion and submission of appropriate CIRS access forms to HR-ISA.
- Determining a user's access to Compendium reports, as well as each ad hoc reporting file, and the available fields within each file.
- Notifying HR-ISA regarding deletion of system users, and changes to hardware and security.
- Conducting a walk-through of the system with new users to determine all functions are operating correctly.
- Disseminating information regarding CIRS to all campus users.

Distribution:

CSU Presidents
Executive Vice Chancellor & CFO
Vice Chancellor, Human Resources
Vice Presidents, Administration
State Controller's Office, Decentralization Security Administrator

Human Resources Directors
Associate Vice Presidents/Deans of Faculty Affairs
Payroll Managers

- Following policies and procedures outlined in the State Controller's Office (SCO) Security Token Agreement and the SCO Decentralized Security Guidelines.

Confidentiality Form Requirement
As referenced in the last bullet above, the SCO Decentralized Security Guidelines require securing the necessary signatures on form PSD108. This is a requirement for users with access to SCO systems such as PIMS **and also is a requirement for CIRS only users**.

Effective immediately, HR-ISA will be storing copies of these PSD108 forms. We have enclosed the SCO guidelines and form for your convenience. At this time, we request that each Security Coordinator have **all** current CIRS users review the SCO Decentralized Security Guidelines and complete and sign a new form PSD108. **Please mail signed forms to HR-ISA no later than May 23, 2003 at:**

CSU HR-ISA
300 Capitol Mall, Suite 213
P.O. Box 942850
Sacramento, CA 94250-5878

Please do not fax these forms as they require social security number; our fax machines are not encrypted.

CIRS users who do not have a signed form to HR-ISA by May 23, 2003, will have their CIRS access revoked until the form is received.

For new CIRS users, the signed form for CIRS-only users must be sent to HR-ISA along with the CIRS access forms. Please retain a copy on campus. For users with access to SCO personnel and payroll systems in addition to CIRS, please continue to follow the procedures PPSD has established with regard to the form PSD108.

Questions regarding this technical letter may be directed to either Yvette Zimmerman-Carrie or Cindy Cairns at (916) 323-5694 or via email at **CIRS@calstate.edu**. This technical letter is available on Human Resources Administration's Web site at: **http://www.calstate.edu/HRAdm/memos.shtml**. Thank you.

CR/cac

OFFICE OF THE STATE CONTROLLER

PERSONNEL/PAYROLL SERVICES DIVISION

DECENTRALIZATION

SECURITY

GUIDELINES

Prepared by

Personnel/Payroll Operations Branch
Training Services and Security Section

December 1996

THIS PACKAGE SHOULD BE REPRODUCED TO PROVIDE INDIVIDUAL COPIES TO STAFF

BACKGROUND

The purpose of these guidelines is to define the State Controller's Office (SCO) security requirements for all users of the SCO computer. Any questions or need for more information should be directed first to your Security Monitor or by contacting the Personnel/Payroll Operations Branch Decentralized Security Administrator at (916) 324-5879.

The SCO maintains a dedicated computer that houses numerous systems of records, which contain confidential and sensitive data. Although automation provides valuable information, access to centrally stored machine-readable data increases the risk of unwarranted disclosure of this data. Therefore, SCO restricts such access to those individuals who have a bonafide need and legal justification for such access.

SCO maintains several automated security control systems, which will continue to be modified as needed, or when more sophisticated technology becomes available. However, individuals using or having control over data which is confidential, or data which could become confidential when associated with other data, must understand SCO requirements for handling such information.

Careless, accidental or intentional disclosure of information to unauthorized persons can have far-reaching effects, which may result in civil or criminal actions against those involved in the unauthorized disclosure (please refer to California Penal Code Section 502 and the California Information Practices Act). To reduce this risk, it is necessary for SCO to establish and enforce these requirements for all system users. Please read this document and the attached PSD108, Statement of Understanding, carefully to ensure comprehension before signing the form.

CONTROLLING ACCESS TO CONFIDENTIAL DATA

1. Access is granted to an individual based on four factors:

   a. They must have access to confidential Personnel/Payroll data in order to perform their legal, statutory, government duties. (If applicable, a "Justification Statement" must accompany this document if the individual does not have a classification that denotes their employment is within the Personnel/Payroll area.),

   b. Must be a bonafide employee of the State and specifically of the requesting agency/campus,

   c. Completion of PSD125A, Security Authorization form, signed by the agency/campus security monitor and authorized manager, attesting to the above mentioned factors

   AND

   d. Completion of the "Statement of Understanding," PSD108, acknowledging that the individual has read and understands these guidelines.

2. These factors are reviewed and access is granted by the Decentralized Security Administrator who represents the Chief, Personnel/Payroll Services Operations Branch.

3. Once access has been approved, the individual is assigned a "UserID." The Security Monitor will be contacted by the SCO Information Security Office to arrange processing of a password that will be known only to the individual. This unique password is the essential security system element that protects both the individual and SCO data from unauthorized disclosure.

4. PASSWORDS: the individual owner must protect their password at all times. It is never to be disclosed to or "shared" with anyone. The failure to protect a password may result in a 30-day suspension from access to the SCO Personnel/Payroll system. Any future failure to protect the password may result in permanent removal of access. (It should be noted that these actions are not to be misconstrued as punitive - merely a corrective action and a safety precaution to limit further possible harm to the security of SCO confidential data.) Disciplinary or punitive action is determined on a cases-by-case basis and may be in addition to other legal actions resulting from violating state law.

5. TOKENS: some agencies/campuses are now using personal computers in lieu of terminals. As such, the use of special security devices, called "tokens," are required by SCO to be used for additional access security.

   "Tokens" are assigned to individuals and therefore are to be handled in the same manner as "passwords."

6. CAUTION: an individual may be considered to have "shared" their password if another individual uses an "active" terminal/PC under the following conditions:

   a. An individual, having logged-on, leaves the active terminal/PC for an undetermined timeframe (i.e., break, lunch, meeting) and another individual enters data or a transaction on the active terminal/PC.

   b. Either for "training" purposes or for someone who is waiting for access approval; an individual "logs-on" to allow the other person to key-enter data/transactions.

Once an individual logs-on the system, any and all transactions or data keyed-in under that individual's UserID/password, belongs to that individual - regardless of the circumstances or the legality of the information entered. The liability; however, for any illegal transactions belongs to the owner of the password - not the person who entered the transaction. Therefore, each individual must log-off (deactivate a session) prior to leaving a terminal/PC.

Such liability may result in civil and/or criminal actions and be punishable under Section 502 of the California Penal Code.

RESPONSIBILITY FOR PROTECTING CONFIDENTIAL DATA

The responsibility for protecting confidential and sensitive data residing on the SCO computer system is a shared effort. The SCO has a limited role in the total security effort. Our responsibility encompasses the area of data, telecommunications and access security. The area of access security at the initial point resides with department management selecting and requesting access for an individual that meets the criteria, previously mentioned. SCO will then verify, and if necessary, require justification for an individual that does not appear to meet the criteria. This area, including protection of access (passwords), is fairly straightforward and easily understood.

The area that is not so easily understood, is the level of protection of confidential data that is either viewable on individual video monitors or extracted from a printer from the SCO system. This data, once it is removed or viewable within the Personnel/Payroll Office comes under the total protection and responsibility of the staff and management of that office. It therefore behooves staff and management to know and understand the restrictions on disclosure of confidential information delineated in the California Information Practices Act (1977). Precautions to ensure that all necessary physical security interventions have been implemented is imperative to avoid inadvertent access or disclosure to unauthorized individuals. Any failure in this area could result in violations in which individuals, staff and/or management may be held liable. The SCO has no responsibility or control over the physical security area of the department/campus.

Each individual must be aware of the potential disclosure of confidential data either through unlawful use of a password, unattended active terminal/PC or through inadvertent disclosure. The later problem is usually the result of unauthorized individuals viewing confidential data via a screen or documents left out on a desk. Regardless of the manner of exposure, the individual controlling the documents and/or the physical security of the office is responsible for the violation and any subsequent legal consequences as a result of the disclosure. Therefore, all hard copies (including printouts) of data extracted from the SCO computer system remain confidential, but is to be protected by agency/campus personnel from unauthorized disclosure as stipulated in the California Information Practices Act (1977).

The Office of the State Controller adheres to the regulations and requirements set forth in the California Information Practices Act (1977) as well as the Federal Privacy Act (1974). Each agency/campus staff member accessing confidential personal data is encouraged to read and follow the tenets of both these State and Federal statutes.

TO: Personnel/Payroll Services Division (PPSD)
Training Services and Security Section
PO Box 942850, Sacramento, CA 94250-5878
Attn: Decentralization Security Administrator

FROM:

NAME (TYPE OR PRINT) CAMPUS/DEPARTMENT (Do not abbreviate)

CLASSIFICATION (SECTION, UNIT, OFFICE)

*SOCIAL SECURITY NUMBER

SUBJECT: STATEMENT OF UNDERSTANDING

I hereby acknowledge receipt, reading and understanding of the provisions and restrictions contained in the PPSD DECENTRALIZATION SECURITY GUIDELINES.

I fully understand that violations of the security policies and procedures are subject to disciplinary action and immediate corrective action may result in revocation of access to the Personnel/Payroll System of the State Controller's Office (SCO). Any violation of the California Information Practices Act may also result in criminal and/or civil action.

I also understand that unauthorized access, attempted access or use of any computer systems and/or data of the State of California is a violation of Section 502, of the California Penal Code, and is subject to prosecution.

LEGAL SIGNATURE DATE

*Privacy Statement

The Information Practices Act of 1977 (Civil Code Section 1798.17) and the Federal Privacy Act (Public Law 93-579) require that the following notice be provided when collecting personal information from individuals.

AGENCY NAME: State Controller's Office (SCO)

UNIT RESPONSIBLE FOR MAINTENANCE: Personnel/Payroll Services Division, Training Services and Security Section, 300 Capitol Mall/PO Box 942850, Sacramento, Ca 942850-5878.

AUTHORITY: Security access authority and protection of information, data and physical system assets of the State of California are mandated by: Govt. Code Sections; 11761, 11770(9), 11771 117734; State Administrative Manual Sections 4841.1-4841.7 and the SCO Information Security Manual.

PROVIDING INFORMATION: Providing the social security account number is voluntary in accordance with the Federal Privacy Act (Public Law 93-579). If, however, the social security account number is not provided the SCO will be unable to authorize or provide security access to the SCO Personnel/Payroll System.

PURPOSE: The information you furnish will be used to determine your status as a bonafide state employee of the department/campus submitting this document and to verify eligibility for authorized access to the confidential/sensitive data contained in the SCO Personnel/Payroll System. This information will be used by the SCO to establish security access, authentication, tracking/monitoring and internal system controls to ensure proper use of access codes and enforcement of all security requirements.

ACCESS: The information submitted to the Personnel/Payroll Services Division is confidential and only authorized personnel involved in the security process will be allowed access.

THIS FORM SHOULD BE REPRODUCED AS NEEDED